VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Propustnost a kapacita koncentrátoru technologie LoRaWAN

Throughput and capacity of LoRaWAN technology concentrator

2019 Bc. Jan Macura

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Jan Macura**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Propustnost a kapacita koncentrátoru technologie LoRaWAN
Throughput and Capacity of LoRaWAN Technology Concentrator

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je stanovit reálnou propustnost a kapacitu koncentrátoru (gateway) pro technologii LoRaWAN. Součástí práce bude ověření pomocí simulačního modelu např. v prostředí OPNET Modeler.

1. Proveďte rešerši v oblasti stanovení reálné propustnosti koncentrátoru technologie LoRaWAN.
2. Navrhněte empirický model pro stanovení reálné propustnosti jednoho či více koncentrátorů pro technologii LoRaWAN. Pro stanovení propustnosti bude mj. využita pilotní síť lora.vsb.cz.
3. Navržený model ověřte pomocí simulačního modelu např. v prostředí OPNET Modeler.
4. Výsledky srovnejte a zhodnoťte.

Seznam doporučené odborné literatury:

[1] ADELANTADO, Ferran, et al. *Understanding the Limits of LoRaWAN*. IEEE Communications Magazine, 2017.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Libor Michalek, Ph.D.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2019

prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky 1D16 OSTRAVA

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 26. dubna 2019 .....

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 26. dubna 2019 .....

Rád bych touto cestou poděkoval vedoucímu diplomové práce Ing. Liboru Michalkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této práce.

Abstrakt

Tato diplomová práce pojednává o všech aspektech, která ovlivňují celkovou kapacitu a propustnost LoRaWAN koncentrátoru. V první části je krátký úvod do technologie Low Power Wide Area ve kterém lze najít požadavky a výhody. Další část má za úkol vysvětlení principu fungování LoRaWAN včetně kapitoly popisující projekty, které Loru využívají. Ve třetí části lze nalézt rozpis a detailnější popis jednotlivých paramterů, které omezují provoz LoRaWAN. V předposlední části je popsána praktická část, která má za úkol ověřit teoretické znalosti. V poslední části je pomocí modelu vytvořeného v matlabu ověřeno, zda naměřené hodnoty jsou reálné.

Klíčová slova: diplomová práce, kapacita, koncentrátor, LaTeX, LoRa, LoRaWAN, propustnost

Abstract

This diploma thesis deals with all aspects that affect the total capacity and throughput of LoRaWAN concentrator. In the first part there is a short introduction to the Low Power Wide Area technology in which requirements and benefits can be found. The next part is about explaining the principle of LoRaWAN, including a chapter describing the projects that LoRa uses. In the third part you can find a breakdown and a more detailed description of the individual parameters that limit the operation of LoRaWAN. In the penultimate part is described practical part, which is supposed to verify theoretical knowledge. In the last part, the model created in matlab verifies whether the measured values are real.

Key Words: capacity, gateway, LaTeX, LoRa, LoRaWAN, master thesis, throughput

Obsah

Seznam použitých zkratek a symbolů

ABP	–	Activation by personalization (Aktivace personalizací)
AES	–	Advanced Encryption Standar (Standard pokročilého šifrování)
CR	–	Code Rate (Kódovací rychlost)
CSMA	–	Carrier Sense Multiple Access (Multinásobný přístup naslouchánímnosné)
ČTÚ	–	Český Telekomunikační Úřad
ETSI	–	European Telecommunications Standards Institute (Evropský ústav pro telekomunikační normy)
FSK	–	Frequency-shift keying (Fázové klíčování)
EUI	–	End-device identifier (Identifikátor koncového zařízení)
IoT	–	Internet of Things (Internet věcí)
IEEE	–	Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)
ISM	–	Industrial, scientific and medical (Průmyslové, vědecké a zdravotní)
MAC	–	Media Access Control (Řízení přístupu k médiu)
OTAA	–	Over-the-air activation
QoS	–	Quality of Service (Kvalita služeb)
RSSI	–	Received Signal Strenght Indicator (Indikátor síly přijímaného signálu)
SF	–	Spreading factor (Činitel Rozprostření)
SNR	–	Signal To Noise Ratio (Poměr signál - šum
ToA	–	Time On Air (Délka vysílání)
TTN	–	The Things Network
LPWAN	–	Low-Power Wide-Area network
WAN	–	Wide Area Network

Seznam obrázků

Seznam tabulek

Seznam výpisů zdrojového kódu

Úvod

V dnešní době se začínáme čím dál častěji setkávat se sítí označenou jako IoT (Internet Of Things). Představa, že každé fyzické zařízení dokáže komunikovat a zaznamenávat data přináší velkou výhodu. Myšlenka chytrého města vznikla již dávno, nicméně díky této technologie může být její realizace mnohem jednodušší a cenově přívětivější. Mezi nejčastěji používané technologie v IoT patří LoRaWAN. Její obrovská výhoda spočívá v nízké spotřebě energie a velkému rádiovému dosahu. Tyto výhody jsou zároveň podmínkou IoT sítě.

V první části diplomové práce je uvedeno několik základních informací o technologii LoRaWAN. Dále zde nalezneme také kapitoly o zabezpečení a principech fungování celé sítě. Nechybí zde ani zmínka o již fungujících projektech postavených na technologii LoRaWAN.

Druhá část je více zaměřena na praktickou část celé diplomové práce. Nalezneme zde podrobnější rozpis parametrů, které omezují celou propustnost a kapacitu koncentrátoru, mezi které také platí omezení vydané ČTÚ. Rovněž je kladen důraz na soupis již vytvořených studií na podobné téma. Celá práce je následně ověřována vůči experimentu, který byl vytvořený na Belgické Univerzitě.

1 Low-Power Wide-Area Network

Jednou z nejslibnějších nových technologií řídící technologii Internet of Things (IoT) je technologie Low Power Wide Area Network (LPWAN). LPWAN poskytuje novou alternativu k tradiční komunikaci s buňkami / M2M, která přichází jak v licencovaném kmitočtovém spektru (celulární), tak i v nelicencovaných variantách technologií frekvenčního spektra. Licencované i nelicencované technologie LPWAN slibují nízkonákladové IoT zařízení s dlouhou životností baterie, která mohou rozšířit případy používání IoT a umožnit nasazení IoT v mnohem širším měřítku.

Pro všechny možné aplikace IoT neexistuje pouze jedno řešení, ale nespočet řešení jak v licencovaných a nelicencovaných pásmech. Vzhledem k široké škále případů využití, které IoT bude muset řešit, je rozmanitost řešení a technologií klíčovým požadavkem při zvažování poskytovatele anténního řešení.

LPWAN technologie je určena pro čidla a aplikace, která potřebují posílat relativně malé množství dat na velké vzdálenosti vícekrát za hodinu a z různého prostředí. Tato technologie vyžaduje baterii s několikaletou životností.[1]

Požadavky na LPWAN:

- Precizní síťová architektura
- Velký komunikační dosah signálu
- Nízká spotřeba energie
- Dlouhá životnost baterie
- Odolnost proti rušení
- Zabezpečení sítě na vysoké úrovni
- Jednosměrná komunikace vs obousměrná komunikace
- Možnost využití velkého počtu aplikací

2 LoRa a LoRaWAN

LoRa

LoRa je fyzická vrstva resp. radiová modulace, která se používá pro vytvoření telekomunikačního spojení na velkou vzdálenost.

Starší bezdrátové systémy rovněž využívají modulaci založenou na frekvenčním posunu (FSK), neboť se jedná o velmi účinnou a robustní modulaci. Při nízkém vysílacím výkonu lze dosáhnout spolehlivého přenosu informací.

Systém LoRa je založen na modulaci rozprostřeného spektra, která má velmi podobnou charakteristiku jako FSK modulace, avšak na mnohem větší vzdálenost. Provoz v rozprostřeném spektru se začal používat v armádě již před několika desítkami let, především z důvodu dlouhého dosahu a odolnosti vůči rušení.

LoRa je prvním komerčním řešením s nízkými investičními i provozními náklady a obrovským obchodním využitím. Hlavní výhodou technologie LoRa je její dlouhý dosah. Jedna brána nebo jedna základna může velmi rychle pokrýt i velmi rozsáhlá území, např. celá města nebo stovky kilometrů čtverečních. Celkový dosah této technologie je závislý na překážkách, které musí v prostředí překonat (hustota zastavěnosti, členitost terénu atd.).

LoRa a LoRaWAN mají nejlepší parametry pro navázání spojení ze všech jiných standardizovaných komunikačních technologií. Celkový útlumový budget na spojení je obvykle uváděn v desítkách decibelů (dB). Díky těmto parametrům lze pokrýt celou zemi s minimálním množstvím infrastruktury.[2]

Mezi hlavní výhody patří:

- Nízká spotřeba energie
- Dlouhý provoz na baterii nebo provoz na solární panel
- Velký dosah vysílaného signálu
- Nízké náklady na výstavbu infrastruktury
- Oboustranná komunikace
- Bezpečnost (zprávy jsou šifrovány)

LoRaWAN

LoRaWAN definuje komunikační protokol a síťovou architekturu systému, zatímco fyzická vrstva LoRa umožňuje komunikační spojení na velkou vzdálenost. Protokol a síťová architektura mají největší vliv na životnost baterie, kapacitu sítě, kvalitu služeb, bezpečnost a paletu aplikací použitelných v sítí.

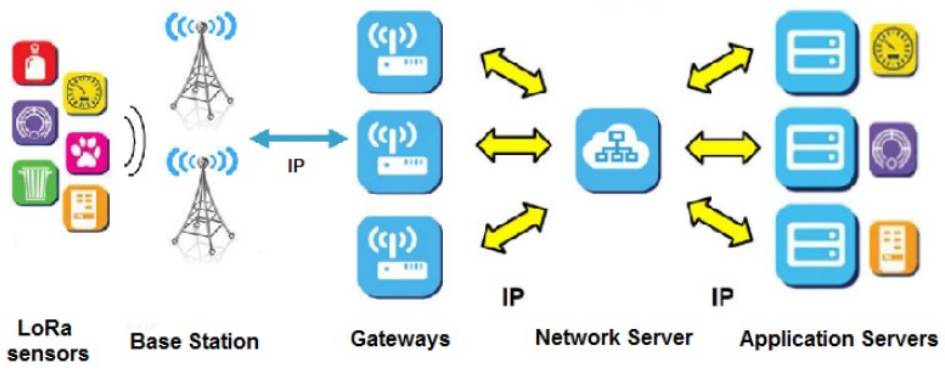
LoRaWAN definuje 10 kanálů. Osm z nich má vícenásobnou datovou rychlost od 250 bps do 5.5 kbps, dále jeden vysokorychlostní datový kanál s rychlostí 11 kbps a samostatný FSK kanál s rychlostí 50kbps. Maximální povolená výstupní úroveň podle ETSI v Evropě je +14dBM s výjimkou 3G pásma umožňující 27dBm. Tyto mají omezení v pracovním cyklu podle ETSI, ale to se nevztahuje na maximální přenos dat nebo dobu setrvání na jednom kanálu.[2]

2.1 Síťová architektura

Long Range sítě využívají architekturu do hvězdy. Tato architektura zajišťuje dlouhou životnost baterie při zachování velkého dosahu sítě.

Základní prvky topologie LoRaWAN dělíme na tři skupiny:

- **Koncové stanice** - senzory s malou spotřebou energie, které komunikují s koncentrátorem (gateway)
- **Koncentrátor** (Gateway) - brána, která propojuje senzory komunikující pomocí protokolu LoRa do internetu
- **Síťové servery** - servery zajišťují dekódování zprávy zaslané senzorem a vytvářejí další zprávy, které jsou zaslány zpět do senzoru



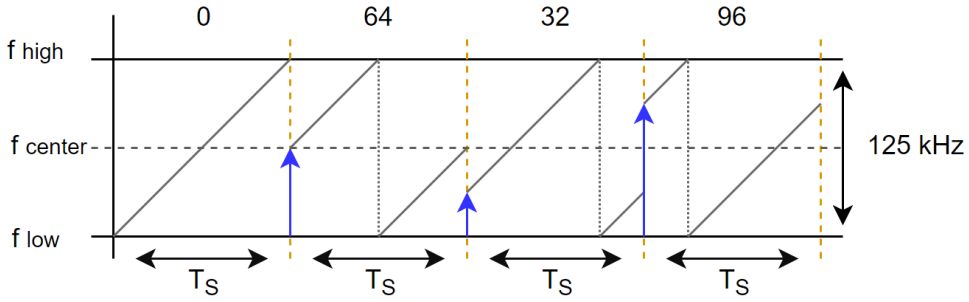
Obrázek 2.1: Topologie sítě LoRaWAN
[3]

2.2 Fyzická vrstva

Základní princip radiové komunikace používané v technologii LoRa je znám již desítky let. Své první uplatnění totiž nalezl při komunikaci s armádními ponorkami.

Základem je lineární frekvenční modulace v kanálu o šířce 125, 250 a 500 kHz, u které se pracuje s tzv. rozprostřeným spektrem.

Užitečná informace je díky redundantnímu až dvanácti bitovému kódu (chirp) přenesena od vysílače k přijímači. Činitel rozprostření může být v závislosti na radiových podmínkách a vzdálenosti (útlumu) dynamicky měněn a pohybuje se v rozmezí 7 až 12. V technologii LoRa je tato hodnota nazývána Spreading Factor (SF). Na základě velikosti SF lze určit počet tzv. chipů, které reprezentují počet bitů, které můžeme modulovat. Na obrázku 2.2 je zobrazena reprezentace decimálních hodnot 0, 64, 32 a 96 při SF = 7.



Obrázek 2.2: Rozprostřené spektrum při SF7

Velikost přenosové rychlosti lze vypočítat dle vzorce 2.1. V tabulce 2.1 lze vidět konkrétní hodnoty přenosové rychlosti při měnícím se činiteli rozprostření.

$$R_b = SF \times \frac{\frac{4}{4+CR}}{\frac{2^{SF}}{BW}} \tag{2.1}$$

SF	Šířka pásma [kHz]	CD	Přenosová rychlost [bps]
7	125	1	5470
8	125	1	3125
9	125	1	1760
10	125	1	980
11	125	1	440
12	125	1	250
Σ			12 025

Tabulka 2.1: Přenosová rychlost logických kanálů

V praxi je použito pásmo 168, 433, 868 a 915 MHz. Jednotlivé pásma jsou rozděleny na 8 kanálů pro vzestupný směr přenosu od čidel a jeden pro sestupný směr k čidlům. Kanál pro směr vysílání od koncového zařízení směrem ke koncentrátoru je zvolen v oblasti spektra, ve kterém je nařízena ČTÚ velikost klíčovacího poměru. Všechna nařízení vydaná ČTÚ lze najít ve všeobecných oprávněních v aktuálním znění – VO-R/10/01.2019-1 [15]

Hodnotu klíčovacího poměru pro různé frekvenční kanály můžeme najít v tabulce 2.2. [15]

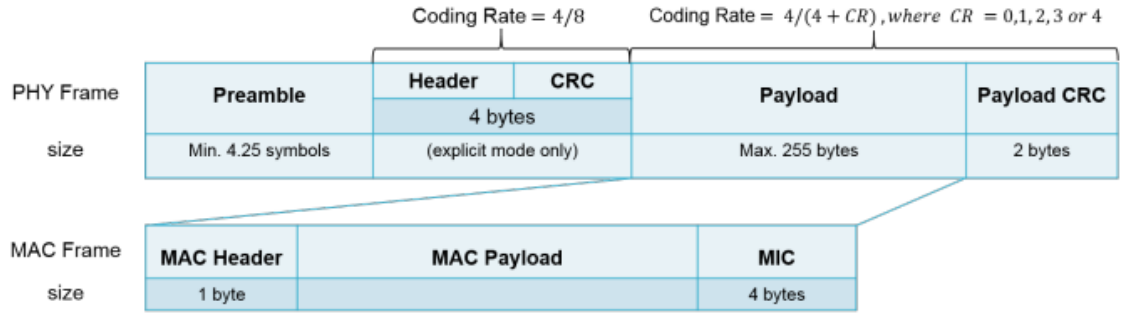
Kmitočtové pásmo [MHz]	Vyzářený výkon	Klíčovací poměr
863,0–870,0	25 mW e.r.p.	0,1%
868,0–868,6	25 mW e.r.p.	1%
868,7–869,2	25 mW e.r.p.	0,1%

Tabulka 2.2: Povolené technické parametry pro kmitočtové rozsahy [15]

Zprávy obsahují záhlaví, ve kterých každé čidlo vysílá své unikátní číslo EUI, které je možno přirovnat k MAC adrese v ethernet sítích. Každá zpráva dále obsahuje své sekvenční číslo. Síť funguje tak, že každá GW, která je v dosahu čidla a zprávu slyší, ji přepošle do network serveru. Na úrovni network serveru se potom podle sekvenčního čísla zprávy odstraňují duplicity, případně se vyhodnocuje, zda nedošlo ke ztrátě předchozí zprávy nebo celé sekvence.

Ve zprávě jsou také zakódovány provozní informace o radiové vrstvě. Na jejich základě lze díky obousměrné komunikaci nejen monitorovat stav čidel, ale také na dálku čidla řídit – změnou činitele rozprostření (spreading factor), doporučovat použitý kanál pro vzestupný směr a regulovat vysílací výkon, což ovlivňuje při hustší infrastruktuře počet koncentrátorů v dosahu signálu a tím eliminovat rušení. Regulace výkonu navíc pozitivně ovlivňuje energetickou náročnost a současně životnost baterií v čidlech.

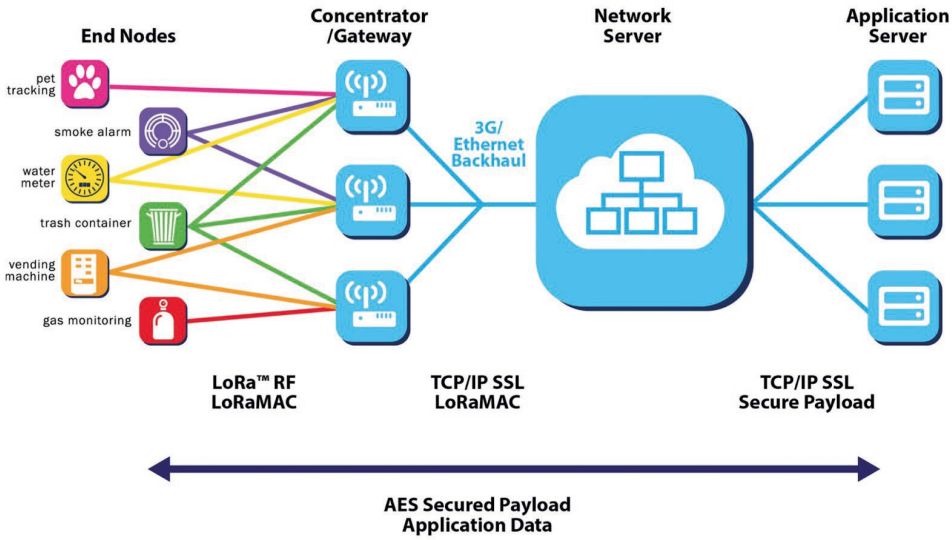
Maximální délka zprávy je 255 bajtů. Tuto délku zprávy lze vysílat pro SF 7-12. Pro vyšší hodnoty SF délka zprávy klesá (což souvisí s dobou vysílání jedné zprávy). Zpráva se zkracuje na úkor možnosti přenášet užitečná data (payload). U zprávy standardní délky 255 bajtů je pro užitečná data 240 bajtů. Při nastavení SF 12 je prostor pro užitečná data 51 bajtů, což je ale pro převážnou většinu čidel stále dostatečná kapacita.[5]



Obrázek 2.3: Struktura LoRa paketu
[4]

2.3 Zabezpečení

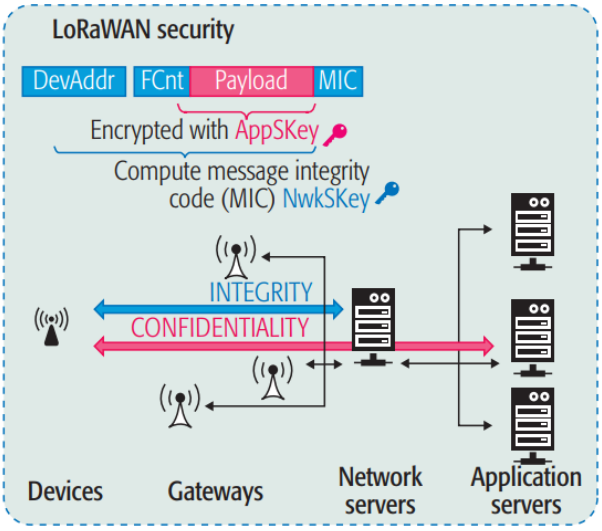
Bezpečnost je pro všechny LPWAN sítě velmi důležitá. LoRaWAN sítě používají dvě bezpečnostní vrstvy – jednu vrstvu pro síť, druhou pro aplikace. Síťovou bezpečnost zajišťuje autentifikace koncového zařízení k jednotlivému síťovému uzlu. Na straně aplikační vrstvy se zajišťuje bezpečnost tím, že network operátor nemá přístup k aplikačním datům uživatele. Aplikační data koncového uživatele jsou navíc zakódována pomocí AES metody používající k výměně klíče IEEE EUI64 identifikátor.



Obrázek 2.4: Ukázka zabezpečení komunikace sítě
[2]

LoRaWan používá dva druhy relačních klíčů:

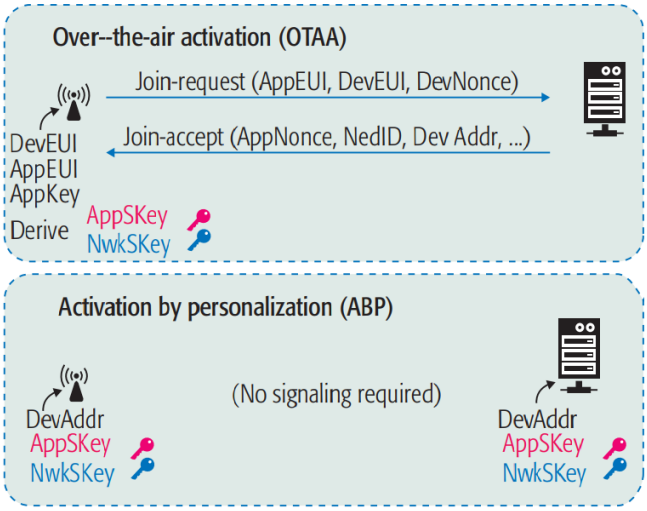
- **NwkSkey** (Network Session Key) - síťový klíč šifruje celou zprávu kromě EUI (Unikátní číslo - ekvivalent MAC adresy v Ethernetu). Šifrováno je tedy kromě payloadu také sekvenční číslo a všechny rádiové informace jako jsou například informace o použitím spreding factoru, použitém kanálu nebo vysílaném výkonu. Toto zajišťuje zabezpečení proti podvrhu čidel a správu těchto klíčů má na starost provozovatel sítě. [7]
- **AppSkey** (Application Session Key) - aplikační klíč narozdíl od síťového šifruje pouze payload (užitečnou informaci). Zajišťuje tím pádem privátnost uživatelských dat. Správu těchto klíčů má na starost provozovatel aplikace. [7]



Obrázek 2.5: Šifrace zprávy pomocí relačních klíčů [6]

Tyto klíče se pak využívají k aktivaci zařízení:

- **OTAA** (Over-the-air activation) - tento typ aktivace při každé spuštěné relaci vygeneruje nový NwkSkey a AppSkey. [7]
- **ABP** (Activation by personalization) - Při této aktivaci se využívají staticky nastavené klíče, které jsou platné do té doby, než je uživatel změní. [7]



Obrázek 2.6: Aktivace zařízení [6]

2.4 Třídy zařízení

Při navrhování specifikací technologie LoRa, byly brány v úvahu různé aplikace, pro které bude možno síť využít. Možností je celá škála a při každé využijeme jiné nároky na způsob komunikace a spotřebu energie. Proto byly vytvořeny 3 třídy zařízení

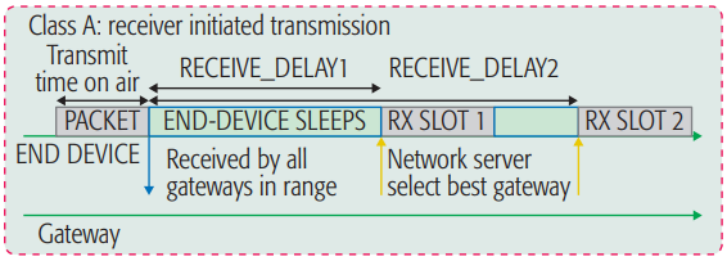
Třída zařízení A

Tato třída byla vytvořena pro případy, kdy není k dispozici přívod napájení a mezi hlavní požadavky patří sběr dat nebo případné ovládání prostřednictvím zasílaní zpráv směrem k čidlu s časovou prodlevou.

Hlavním specifikem této třídy čidel je iniciování komunikace stranou čidla a to na základě události, kterou chceme detekovat (např. detekce kouře u kouřového čidla nebo změna měřené veličiny) a nebo na základě časového intervalu, který je nastavený v časovači ukrytého v čidle.

Princip odesílání zprávy je tvořen dvěma intervaly o celkové délce trvání 2 sekundy, během kterých je čidlem očekáváno doručení zprávy, díky které lze provést konkrétní akci (sepnutí či vypnutí ovládaného obvodu, přenastavení časového intervalu atp.)

Ideální využití zařízení třídy A je například měření spotřeby vody nebo plynu v místech, kde nemáme k dispozici stabilní napájení. Lze také využít schopnost připojení či odpojení zařízení na dálku. Toto lze využít například při vytápění objektu v době kdy je za energie účtovaná nižší sazba atp. [5]



Obrázek 2.7: Popis vysílání zařízení třídy A
[6]

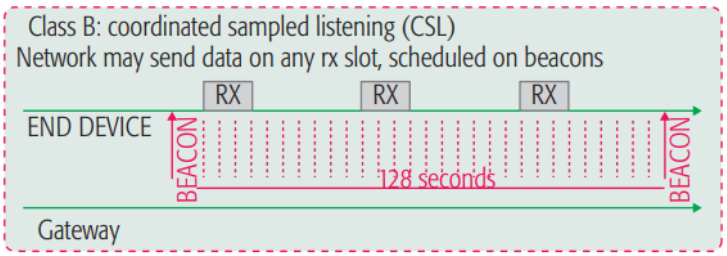
Třída zařízení B

Použití pouze čidel třídy A není vyhovující pro spoustu uživatelských aplikací, u kterých je nutná obousměrná komunikace.

Příkladem může být pohybové čidlo nebo dveřní kontakt v zabezpečeném objektu. Ideální využití pro zabezpečení je v odlehlých např. technologických prostorách, kde není dostupné napájení a četnost vstupů není příliš vysoká. U takových aplikací je totiž třeba přepínat mezi stavy střeženo a nestřeženo. Čidla třídy A jsou nevhodná, protože potřebujete v poměrně krátkém intervalu změnit režim provozu. Lze to sice zajistit nastavením časovače na krátký opakovací interval, to však zbytečně zatíží síť a zejména se tím popře nízká energetická náročnost.

Třída zařízení B představuje kompromis v možnosti přijímat zprávy v libovolném okamžiku anebo v závislosti na události vzniklé v čidlu třídy A. Rozdíl oproti třídě A spočívá v tom, že jsou čidla nastavena tak, že v pravidelném časovém intervalu aktivují svou přijímací radiovou část, aniž by došlo k vysílání zprávy (což představuje pro čidlo energeticky nejnáročnější operaci).

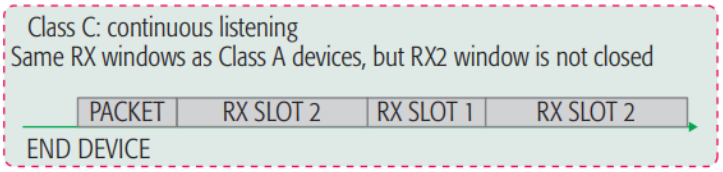
Režim provozu nazývaný vědecky jako koordinovaný vzorkovací poslech spočívá v tom, že se sítí šíří tzv. beacony – synchronizační impulsy s intervalem 128 sekund, které slouží k tomu, aby si interní časovače čidel srovnaly svá nastavení v souladu se síťovou synchronizací.



Obrázek 2.8: Popis vysílání zařízení třídy B
[6]

Třída zařízení C

V případech, kde není třeba řešit nízkou energetickou náročnost, mohou být použita čidla třídy C, u kterých je přijímací část čidla trvale aktivována a ovládací zpráva ze sítě tedy může být přijata v libovolném časovém okamžiku. Typický případ použití čidel třídy C je například u „chytrých elektroměrů“ nebo aktuátorů sloužících k připojování/odpojování energetických celků nebo strojů a zařízení, u kterých je požadována okamžitá odezva.[5]



Obrázek 2.9: Popis vysílání zařízení třídy C
[6]

2.5 Projekty postavené na technologii LoRaWAN

Tato kapitola popisuje realizované projekty využívající technologii LoRaWAN. Projektů stále přibývá a to hlavně díky nízké ceně a jednoduchosti. Existuje také celá řada domácích výtvorů, které lze najít právě na webu TTN v sekci Labs. Většina těchto výtvorů má ve svém popisu i detailní návod, který může posloužit jako inspirace pro vytvoření podobného projektu.

Smart mouse trap

Jedná se o jednoduchou chytrou past na myši či krysy. Tento výrobek byl vytvořen firmou Xignal sídlící v Nizozemsku. Princip je velice jednoduchý, po té co past chytí hlodavce, vyšle zprávu, která je následně uložena na server, kde můžeme zpracovávat jednotlivé reporty. Díky nízké spotřebě baterie lze tyto pastičky rozmístit i do míst, kde není možné připojit senzor k napájení. [11]

Aelora

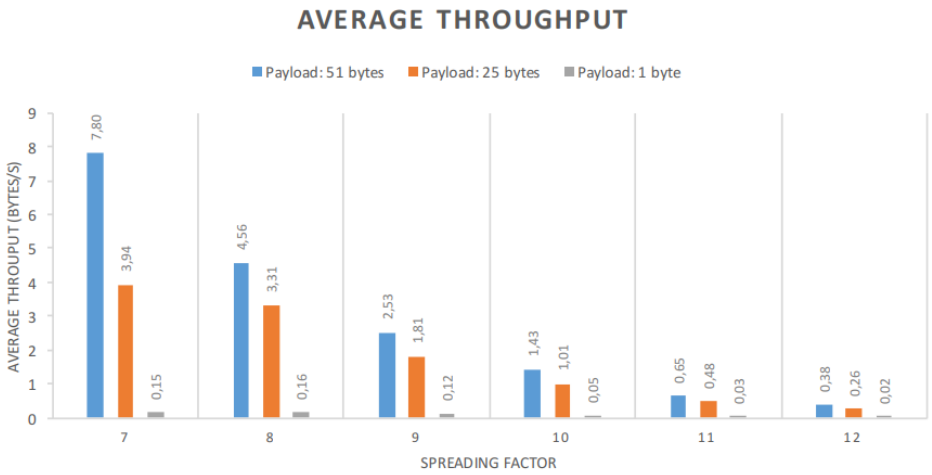
Tento projekt využívá k měření kvality ovzduší technologii LoRaWAN společně s The Things Network. Celý koncept byl vytvořen čtyřmi kolegy: Fokke Zandbergen, Richard van der Laan, Jacco Schouw a Ivo Domburg. Celá infrastruktura je postavená z Arduino Nano a LoRa modulem RN2483. Hardware je uschován do velice originální sošky oranžového ptáka vytvořeného pomocí 3D tiskárny.[12]

Obrázek 2.10: Aelora senzor [12]

Data ze senzorů putují na web TTN, kde pomocí MQTT brokeru dochází ke stažení dat do databáze, která je přístupná pomocí webové stránky aelora.nl. Na tomto webu se nachází podrobná mapa s lokacemi senzorů. Každý senzor dokáže zobrazit naměřená data.

3 Rešerše v oblasti propustnosti a kapacity LoRaWAN koncentrátoru

Jeden z nalezených experimentů si kladl za cíl vyhodnotit maximální propustnost, kterou může jediné zařízení dosáhnout. V tomto případě záleží více na fyzické vrstvě nežli na MAC protokolu. Zařízení odesílalo data okamžitě, jak to jen omezení kanálu a protokol dovolil. Test byl prováděn na šesti kanálech o šířce 125 kHz a používal se rozprostřený faktor od 7 do 12. Během testování nebyly zasílány žádné MAC příkazy a tím pádem velikost MAC hlavičky byla konstantních 13 bytů. Výsledek byl tím pádem závislý pouze na velikosti užitečné zprávy, neboli payloadu. Tomu byla zvolena velikost 51, 25 a 1 byte. V každém testu bylo posláno 100 paketů. Na obrázku 3.1 lze vidět, jak se propustnost lišila při použití různých hodnot rozprostřeného faktoru.[8]



Obrázek 3.1: Maximální propustnost jednoho zařízení používající LoRaWAN [8]

Tento experiment ukázal, že při malých velikostech paketů nejsou omezujícím faktorem pravidla kanálu či omezení cyklů, ale doba trvání přijímacích oken. Zařízení musí počkat na dva sestupné přijímací okna přenostu, která musí být ukončena před odesláním dalšího paketu. Tento fakt nicméně pro fungování LoRaWAN není důležitý. Tato síť byla konstruována pro správu velkého množství zařízení, které posílá několik bytů čas od času.

Další faktor, který byl jiný nežli v případě reálném provozu byla velikost MAC hlavičky, která v našem případě byla 13 bytů. Tato velikost není v reálném provozu konstantní, ale může nabývat velikosti od 13 do 28 bytů. Navíc celková velikost rámce je závislá na použité datové rychlosti. LoRaWAN nepoužívá žádný mechanizmus na rozdělení velké užitečné datové části na více rámců. Nemá ani žádný způsob jak zjistit jaká bude maximální velikost paketu, který bude zaslán v příštím přenosu, což může být problematické. Řešením může být posílání pouze

velikosti rovnající se nejmenší možné velikosti payloadu což je 36 bytů což vede k zmenšení celkové kapacity koncentrátoru. [8]

3.1 Maximální kapacita a zatížení kanálu

Celková kapacita sítě není závislá pouze na velikosti payloadu. Dvě vysílání o stejné frekvenci a rozdílném rozprostřeném faktoru můžou být dekódovány současně pouze v případě, že je logický kanál definován frekvenčním pásmem a rozprostřeným faktorem.

Celková přenosová kapacita LoRaWAN sítě se rovná součtu kapacit všech logických kanálů. Například v 125 kHz frekvenčním pásmu můžeme mít šest rozprostřených faktorů (od 7 do 12) což přináší celkovou kapacitu 12,025 bps. Přenosové kapacity pro jednotlivé SF lze vidět v tabulce 2.1. K vytvoření tabulky byl použit vzorec 2.1 Když vezmeme v potaz, že v EU máme tři takové to pásma, celková kapacita sítě je 12,025 x 3 = 36 kbps. [8]

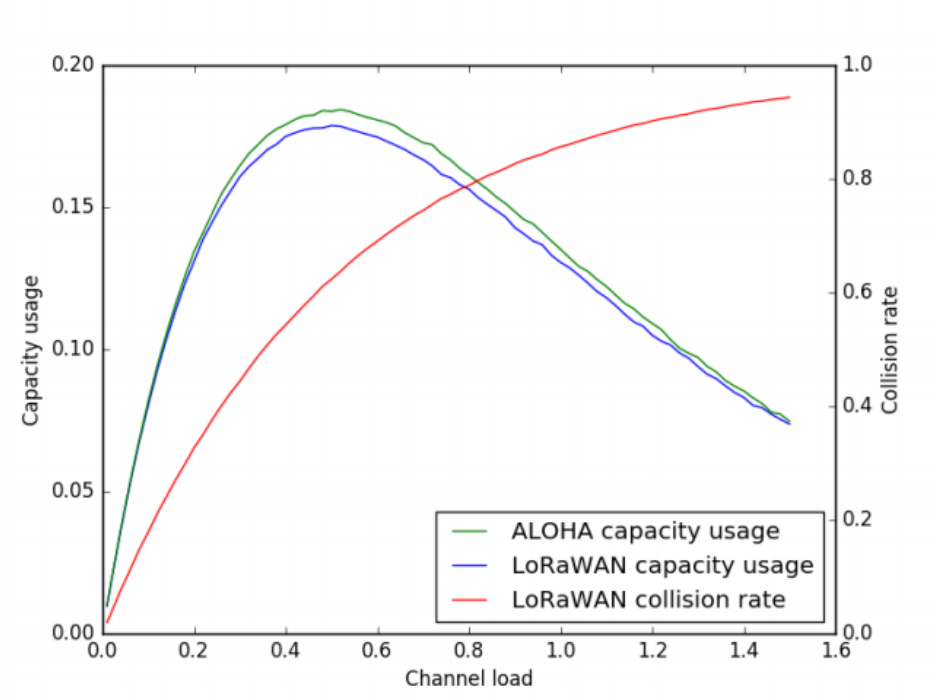
Vzhledem k faktu, že přenosová rychlost je závislá na použitém rozprostřeném faktoru, nemají logické kanály stejné kapacity.

3.2 Odhad počtu kolizí

Jak již bylo psáno výše, zařízení a koncentrátor mohou vysílat kdykoliv. To přináší kolize v případě, že dva zařízení vysílají zároveň. Kolize jsou řešeny v LoRaWAN dvěmi způsoby a to listen-before-talk nebo metoda CSMA. Tedy LoRaWAN je velice podobná metodě ALOHA, kdy nepotřebujeme žádný řídící prvek pro kontrolu vysílání, ale zařízení se samo snaží odhadnout situaci v provozu sítě. Nicméně LoRaWAN na rozdíl od metody ALOHA využívá proměnné délky rámců.

Při psaní článku o nějž se opírám byl vytvořen simulátor, který čítal 5000 paketů pro každé zařízení. V případě, že docházelo k vysílání ve stejný čas, došlo ke kolizi a ani jeden z paketů nedorazil ke koncentrátoru. Výsledná hodnota kolizí byla pak rovna poměru přijatých paketů vůči všem odeslaným paketům. Využití kapacity kanálu se vyhodnocuje z množství úspěšně přijatých dat v průběhu simulace, které se podělilo maximálně možným množstvím dat, které by mohly být odeslány v jednom kanálu.

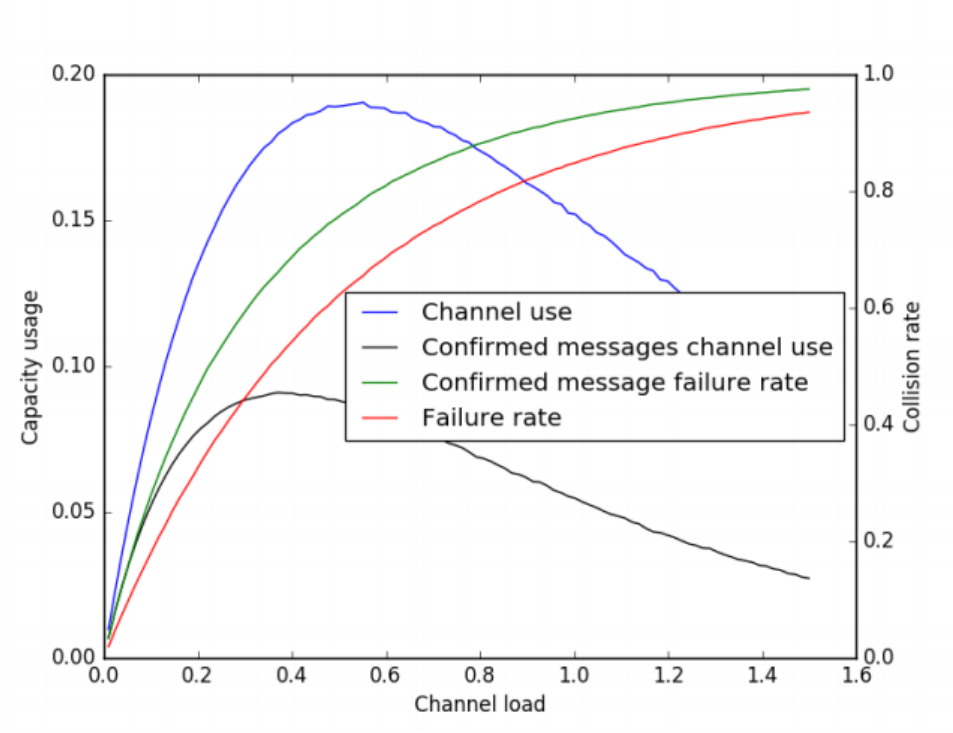
Výpočet délky paketu pro různé velikosti payloadu probíhal za pomocí LoRa kalkulačky od společnosti Semtech. Rozprostřený faktor byl nastaven na hodnotu 7 a šířka pásma byla klasicky 125 kHz. Hodnota payloadu se pohybovala mezi 1 až 51 bytů.[8] Závislost kapacity využití a velikosti kolize na vytížení kanálu lze vidět na grafu 4.2



Obrázek 3.2: Závislost velikosti kolize na vytížení kanálu
[8]

Nyní se při výzkumu zaměřili na potvrzované zprávy, které při odeslání zařízením musí být potvrzeny odesláním paketu během jednoho ze dvou přijímaných oken po přenosu na rozdíl od zprávy, které jsou odeslány koncentrátorem. Tam stačí k potvrzení pouze příznak v hlavičce paketu.

Hlavní nevýhodou tohoto principu je to, že potvrzená zpráva potřebuje dvě po sobě jdoucí úspěšné zprávy což zvyšuje pravděpodobnost další kolize a tím i počet opakovaných vysílání. Jako u předchozích simulací nebyly vysílaný žádné MAC příkazy a tím pádem MAC hlavička byla konstantní velikosti 13 bytů. [8] Výsledek simulace můžete vidět na grafu 3.3



Obrázek 3.3: Závislost velikosti kolize na vytížení kanálu při použití potvrzování [8]

Výsledek dopadl dle očekávání, při potvrzování zpráv dochází ke kolizi výrazně častěji než-li v případě vysílání bez potvrzování. Také je zřejmé, že LoRaWAN je citlivá na zatížení kanálu stejně jako je tomu v případě ALOHY. Pokud bychom nemuseli řešit omezení provozním cyklem, dalo by se kolizím zabránit díky zmenšení vysílání ve velkém množství za krátký čas.

Současná verze LoRaWAN nemá specifikované žádné QoS a tím pádem negarantuje kvalitu či jistotu při vysílání. Není tedy vhodná pro využívání kritických aplikací, kde je velice důležité aby zpoždění bylo co nejmenší. [8]

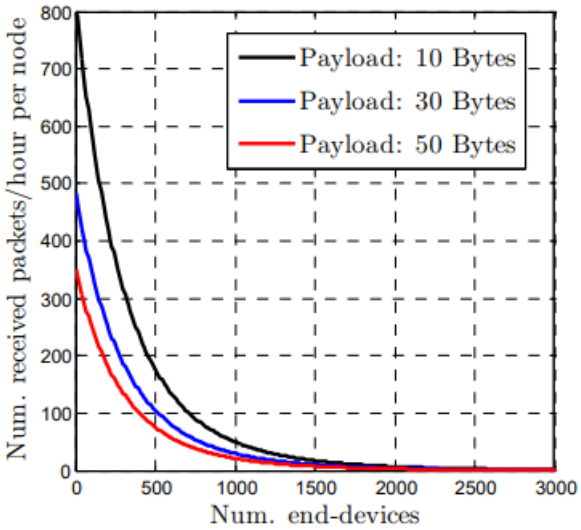
3.3 Studie zabývající se limity a kapacitou sítě LoRaWAN

Z důvodu poměrně nové technologie existuje pouze několik studií, které se zabývají určením limitů LoRaWAN koncentrátoru. V této práci byly tyto studie použity pro ověření naměřených hodnot.

Understanding the Limits of LoRaWAN

Pro zjištění limitů LoRaWAN koncentrátoru posloužilo ověření počtu přijatých zpráv při měnícím se počtu zařízení. Při změně zařízení také docházelo ke změnám velikosti užitečné zprávy

a to na 10, 30 a 50 bytů. Z počtu přijatých zpráv se poté vytvořil poměr vůči odeslaným zprávám. Výsledky můžete vidět na grafu 3.5. Experiment došel k závěru, že nejvíce limitující jsou vznikající kolize při hustém provozu či při dlouhém ToA u zpráv s velkým SF či payloadem. [9]



Obrázek 3.4: Poměr přijatých zpráv vůči odeslaným [9]

Understanding collisions in a LoRaWAN

V tomto experimentu bylo detailněji zkoumáno jak dochází ke kolizím a co se při tomto stavu děje. Během testování proběhla simulace pro jeden i více koncentrátorů v síti.[17]

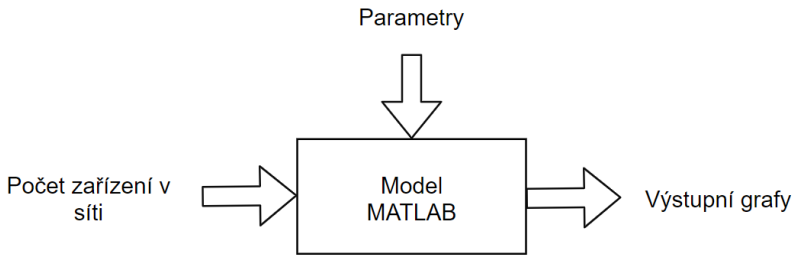
Při kolizi může docházet k:

- Ztracení obou kolidujících zpráv - Nastává v případě, když je slabší signál narušen silnějším v době příjmu.
- Příjmu zprávy se silnějším signálem - Nastane v případě, když silnější zpráva se překrývá s CRC hlavičkou slabší zprávy. Díky tomu koncentrátor odemkne zámek a začne poslouchat novou zprávu.
- Ztracení obou kolidujících zpráv - Nastane v případě, když se překrývá záhlaví silnější a slabší zprávy.
- Ztracení obou kolidujících zpráv - Nastane v případě, když silnější zpráva dorazí v příjmacím okně slabší zprávy. Slabší zpráva je sice úspěšně přijata, její payload, ale bude poškozen.

LPWAN simulation

Největší přínos pro tuto práci přinesl experiment vytvořený Maarten Weyn na belgické univerzitě University of Antwerp. V rámci jeho práce vznikl simulační skript v software matlab, který zkoumá vliv počtu zpráv a velikosti zpráv na počet úspěšně doručených zpráv. Hlavním cílem experimentu bylo srovnání technologie LoRaWAN vůči Sigfoxu.[18]

Níže lze vidět ukázku cyklu FOR, který tvoří hlavní část programu pro simulaci provozu v síti LoRaWAN. Pokud se na kód zaměříme detailněji, zjistíme, že se jedná o jednoduchý cyklus ve kterém jsou vytvořeny náhodné časy s náhodnými stavy - vysílá x nevysílá. Pokud se při kontrole časového okna setká vysílání více zařízení najednou, dojde k zaznamenání kolize do matice, která se následně vykreslí do grafu.



Obrázek 3.5: Schéma simulačního modelu

```
sf = randi([start_channel end_channel], [nr nrofpackets]);
  %time = randi([1 floor(nrofslots - (packetduration*nrofpackets)/
      timeinterval)], [nr 1]);
  for i = 1:nr
      time_offset = floor((nrofslots - (packetduration(sf(i))*nrofpackets)/
          timeinterval) * rand(1,1));%time(i, 1);
      for p = 1:nrofpackets
          for k~= 0
              if (sf(i, p)+k<1) | (sf(i, p)+k>nrofchannels)
                  continue
              end
              duration = lora_duration(sf(i, p),3);
              for j = 1:duration/timeinterval
                 %freq(i, 1)
```

```
                if j+time_offset > nrofslots
                    continue
                end

                if  ft(j+time_offset, sf(i, p)+k) == 0
                    ft(j+time_offset, sf(i, p)+k) = 1;
                    ft2(j+time_offset,sf(i, p)+k) = i;
                else
                     ft(j+time_offset, sf(i, p)+k) = ft(j+time_offset, sf(i, p
                         )+k) + 1;
                     colission(i) = 1;
                     colission(ft2(j+time_offset,sf(i, p)+k)) = 1;
                end
            end
        end
        time_offset = ceil(time_offset + duration/timeinterval);
    end

end

results(floor(nr/devicestepsize), 1) = sum(sum(colission));
results(floor(nr/devicestepsize), 2) = 100*sum(sum(colission))/nr;
fail = sum(colission, 2) == nrofpackets;

if (results(floor(nr/devicestepsize), 2) < 5)
   fiveperc = nr;
end

end
```

Výpis 3.1: Ukázka Matlab skriptu

4 Parametry omezující propustnost LoRaWAN

Tato část diplomové práce se zabývá parametry, které jsou závislé na výsledné kapacitě koncentrátoru LoRaWAN.

4.1 Time On Air

Díky této hodnotě můžeme určit jak dlouhé bude čekání mezi jednotlivým vysíláním, aby nebyla porušena podmínka klíčovacího poměru. Pokud máme určeno, že klíčovací poměr je 1%, tak doba čekání na další vysílání bude 99% z hodnoty Time On Air. Výpočet času lze vidět ve vzorci 4.2 kde T_s je doba jednoho symbolu, $n_{preamble}$ je velikost začátku hlavičky paketu, která se využívá pro synchronizaci. Na obrázku 2.3 lze vidět jednotlivé parametry ve struktuře paketu. [**?**]

$$ToA = T_{packet} = T_{preamble} + T_{payload} \tag{4.1}$$

$$ToA = T_{packet} = T_s \times (n_{preamble} + PLSymb + 4.25) \tag{4.2}$$

$$T_s = \frac{1}{\frac{BW}{2^{SF}}} \tag{4.3}$$

$$PLSymb = 8 + max(ceil(\frac{8PL - 4SF + 288 + 16CRC - 20H}{4(SF - 2DE)})(CR + 4), 0) \tag{4.4}$$

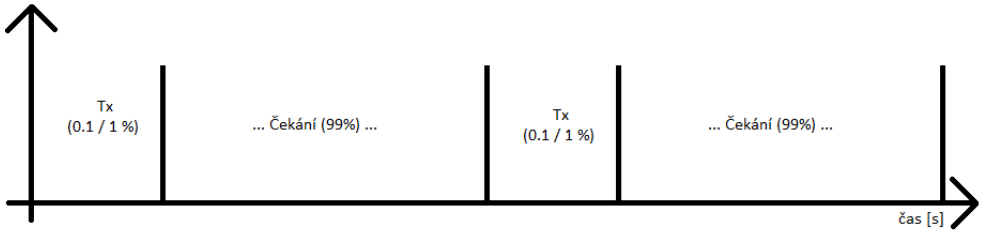
Vysvětlení jednotlivých parametrů použitých ve vzorci 4.4 naleznete níže:

- ToA: Čas během kterého je paket přenesen od zařízení ke koncentrátoru
- $T_{preamble}$: Čas přenosu hlavičky paketu
- $T_{payload}$: Čas přenosu užitečné informace paketu
- $n_{preamble}$: Počet symbolů v hlavičce, pro pásmo EU868 $n_{preamble} = 8$ symbolů
- PL: hodnota playload v bytech
- H: nabývá hodnoty 0, pokud je použita hlavička nebo hodnoty 1 v případě nepoužití hlavičky
- DE: hodnota 1 v případě použití nízkého přenosu dat a 0 v případě klasického přenosu
- CR: Code Rate

4.2 Klíčovací poměr

Klíčovací poměr, také lze nalést pod anglickým názvem duty cycle, je parametr, který nám říká, jak dlouho zařízení může vysílat v daném frekvenčním pásmu. Udává se v procentech a jeho velikost je regulována ČTÚ. Velikost klíčovacího poměru pro různá frekvenční spektra lze najít ve všeobecných oprávněních VO-R/10/01.2019-1. [15]

V pásmu 868 MHz, které využíváme v České Republice je velikost klíčovacího poměru 1%. [14]Což si můžeme představit tak, že ToA zprávy zaslané senzorem je 1% časového okamžiku za kterým následuje 99% čekání. Pokud například vyšleme zprávu o velikostí payloadu 23B a SF8 bude ToA = 113,72 ms. Pokud ToA vynásobíme číslem 99, vznikne nám doba časového okna ve kterém zařízení musí počkat na vyslání další zprávy. V našem případě to bude 11,26 s. Jednoduše lze tedy říci, že čím vyšší bude vysílací doba zařízení, tím vyšší bude i doba čekání na zaslání nové zprávy.



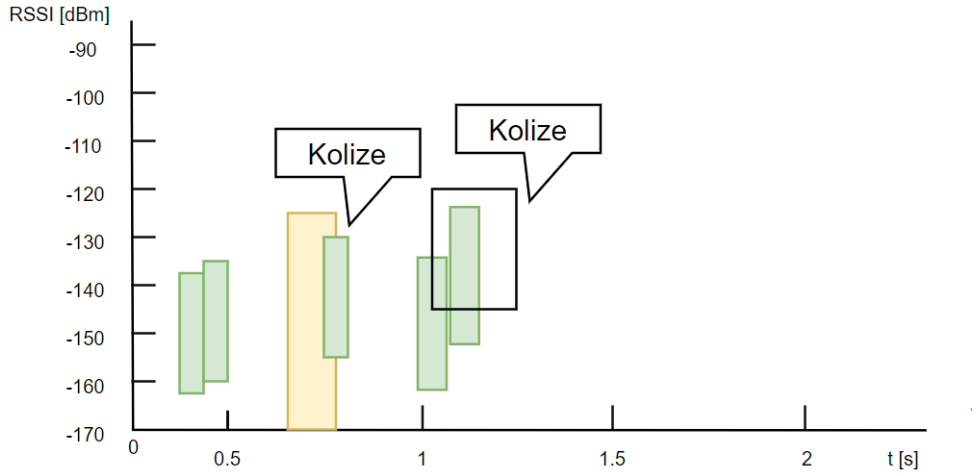
Obrázek 4.1: Grafické znázornění duty cycle

4.3 Kolize

Při zvyšujícím se Time On Air dochází také ke zvyšování pravděpodobnosti kolize a zmenšování propustnosti koncentrátoru. Na obrázku 4.2 lze vidět, že v případě příjmu signálu není koncentrátor schopný přijmout další zprávy.

Obecně lze tedy říci, že v případě použití vyšší hodnoty SF a větší velikosti payloadu, dojde ke zvýšení pravděpodobnosti kolize. Čím vyšší je ToA, tím větší je časové okno ve kterém není koncentrátor schopen přijmout další zprávy a dochází ke kolizím.

Pro snížení počtu kolizí je v technologii LoRaWAN použit přístupový protokol prostá ALOHA.



Obrázek 4.2: Ukázka kolizí při větším ToA

LoRaWan rozlišuje více druhů kolizí:

- **SFn to SFn** (stejná hodnota SF u obou zpráv) - pokud je jedna zpráva o 5 dB silnější tak dojde k úspěšnému přijetí.
- **SFn to SFm** (rozdílná hodnota SF u obou zpráv)

Pokud nenastane ani jedna z podmínek, dochází k zahození obou zpráv v kolizi.

ALOHA

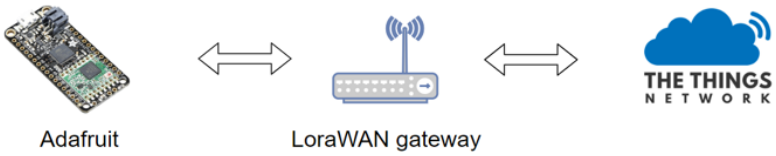
ALOHA je jednoduchý přístupový protokol, který byl vytvořen na univerzitě v Hawaii v roce 1970. Hlavní úlohou ALOHA protokolu je určit čas, kdy se může stanice pokusit opět o přístup ke kanálu. [10]

Mezi pravidla protokolu patří:

- Stanice mohou kdykoliv vysílat
- Neexistuje mechanismus, který by snímal provoz na síti
- Může docházet ke kolizím
- Neexistuje žádná detekce kolize, pouze potvrzování
- Snížení počtu odeslaných zpráv z důvodu náhodného čekání po kolizi

5 Návrh empirického modelu pro stanovení kapacity LoRaWAN koncentrátoru

Při návrhu empirického modelu byl kladen důraz na ověření teoretických výpočtů. Celá sestava byla nastavovat tak aby co vliv parametrů co nejvíce ovlivňovala hodnotu kolizí a tím celkovou kapacitu koncentrátoru LoRaWAN.

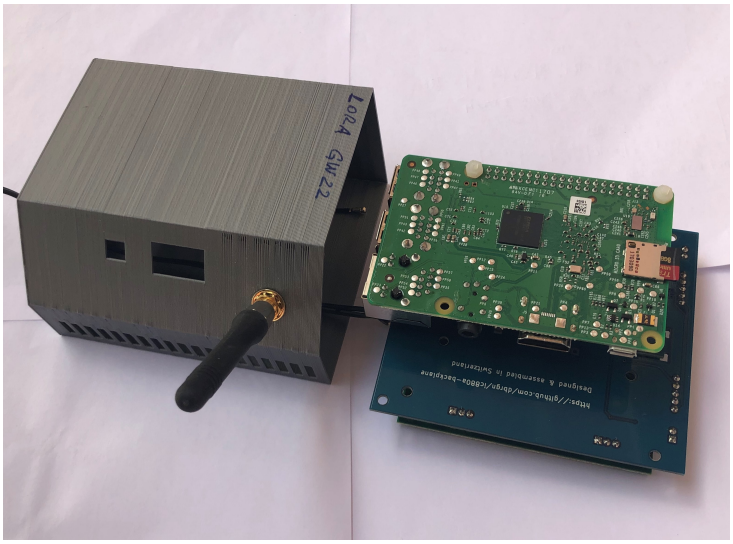


Obrázek 5.1: Schéma empirického modelu

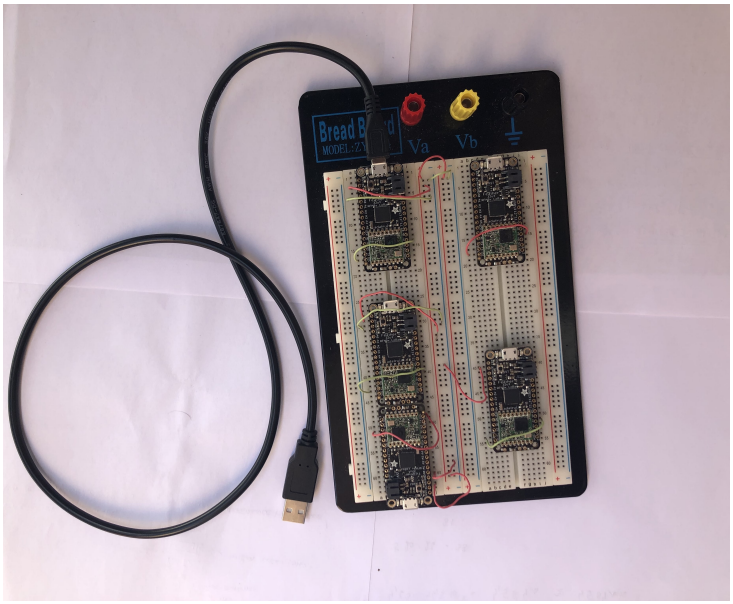
5.1 Hardware empirického modelu

Pro ověření teoretických výpočtů posloužil zapůjčený LoRaWAN koncentrátor který je využívám v nově vybudované síti LoRa VSB. Hardware koncentrátoru byl uložen v krabičce vytvořené na 3D tiskárně. Na straně vysílací nalezneme pět čipů Adafruit.

- Koncentrátor - Raspberry-Pi2B + iC880a SPI
- Koncové zařízení - 5x Adafruit Feather 32u4 RFM9x 5.3



Obrázek 5.2: LoRaWan koncentrátor



Obrázek 5.3: Testovací soustava čipů Adafruit

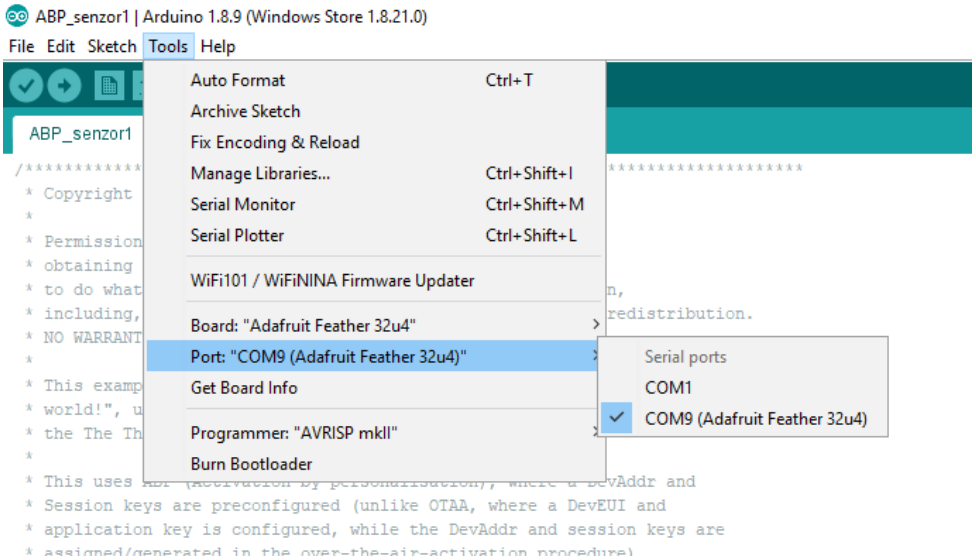
Na obrázku 5.3 lze vidět zapojení čipů Adafruit. Napájení čipů bylo realizováno pomocí MicroUSB kabelu zapojeného do počítače.

Všechny čipy byly propojeny na nepájivém poli z důvodu synchronizace napájení a propojení pinů pro vysílání zpráv. Díky synchronizaci napájení docházelo k vysílání zpráv těsně u sebe a docházelo častěji ke kolizím. Všem senzorům byl následně nastaven stejný statický frekvenční kanál pro další zvýšení pravděpodobnosti kolize.

Programování zařízení

Programování zařízení Adafruit probíhá pomocí aplikace ArduinoID. Zařízení se připojí k PC pomocí MicroUSB kabelu, následně se v aplikaci vybere příslušný port na kterém zařízení naslouchá. K programování se využívá doinstalovaná knihovna LMIC, která byla vytvořena pro účely LoRaWAN.

Knihovna obsahuje i ukázky kódu například pro jednoduché zaslání zprávy pomocí aktivace ABP nebo OTAA. Tento ukázkový kód byl použit pro mé potřeby testování. Na ukázkách kódů níže lze vidět jak nastavit jednotlivé klíče pro úspěšnou aktivaci zařízení vůči aplikaci na serveru TTN.



Obrázek 5.4: Připojený čip do aplikace ArduinoIDE

```
// LoRaWAN NwkSKey, network session key
static const PROGMEM u1_t NWKSKEY[16] = { 0x7D, 0x7D, 0x26, 0x1A, 0xF7, 0xB0, 0
    xE9, 0xC3, 0xC1, 0xEE, 0xF0, 0x67, 0xA8, 0x1B, 0x7E, 0x00 };

// LoRaWAN AppSKey, application session key
static const u1_t PROGMEM APPSKEY[16] = { 0x2F, 0x3E, 0x38, 0x82, 0x24, 0x08, 0
    xDD, 0x72, 0xF2, 0x54, 0x96, 0x8A, 0x26, 0x7F, 0x45, 0xED };

// LoRaWAN end-device address (DevAddr)
static const u4_t DEVADDR = 0x26011EDA ;
```

Výpis 5.1: Ukázka nastavení příslušných klíčů pro ABP aktivaci

```
// little-endian format
static const u1_t PROGMEM APPEUI[8]= { 0xC5, 0x81, 0x01, 0xD0, 0x7E, 0xD5, 0xB3
    , 0x70 };
void os_getArtEui (u1_t* buf) { memcpy_P(buf, APPEUI, 8);}

// little endian format
```

```
static const u1_t PROGMEM DEVEUI[8]= { 0x8C, 0x2D, 0xB9, 0x57, 0xFB, 0x6C, 0xC8
    , 0x00 };
void os_getDevEui (u1_t* buf) { memcpy_P(buf, DEVEUI, 8);}

// big endian format
static const u1_t PROGMEM APPKEY[16] = { 0xAE, 0x02, 0x2E, 0x25, 0x5C, 0xAC, 0
    xF7, 0x2B, 0xBE, 0xD7, 0xE6, 0x74, 0x0A, 0xCC, 0x8D, 0xA4 };
```

Výpis 5.2: Ukázka nastavení příslušných klíčů pro OTAA aktivaci

Knihovna LMIC dále umožňuje různé nastavování frekvencí či SF dle potřeb uživatele. Pro omezení vysílání pouze na jedné frekvenci nebo s určitým SF stačí krátká podmínka for.

```
    for (int i=0; i<9; i++) {
    if(i != channel) {
      LMIC_disableChannel(i);
     }
    }
```

Výpis 5.3: Omezení vysílání na jeden frekvenční kanál

```
int channel = 0;
int dr = DR_SF7;
```

Výpis 5.4: Nastavení konstantního SF

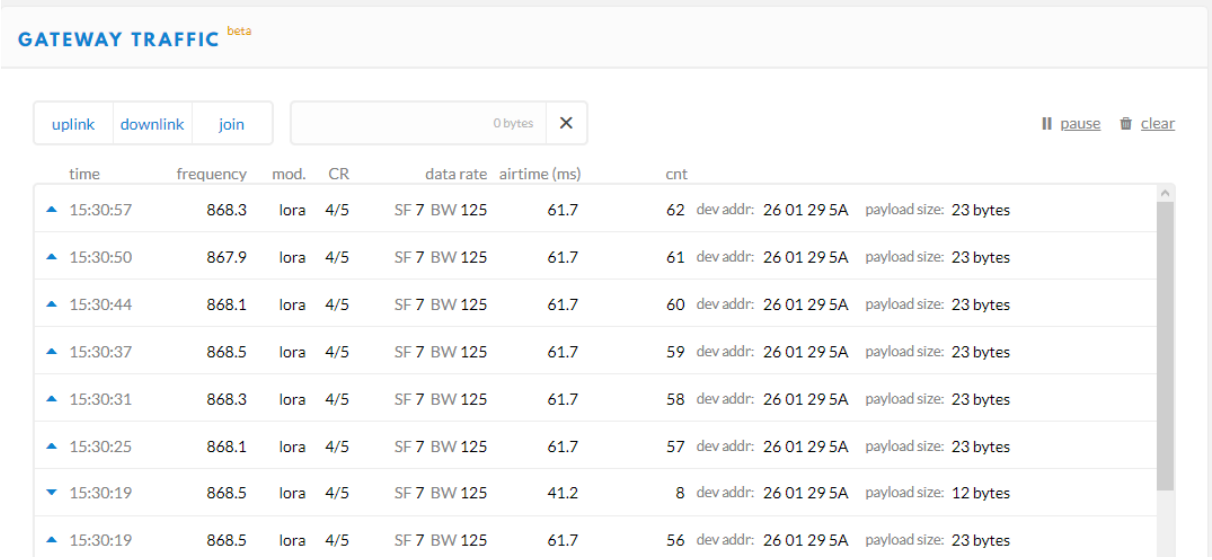
5.2 Popis přístupu k datům

The Thing Network - TTN

Praktické testování probíhalo pomocí konzole na webu The Thing Network. Po zaregistrování lze k účtu přiřadit koncentrátor, který uživatel bude spravovat. Toto přiřazení provedl vedoucí práce.

Obrázek 5.5: Podrobnosti o koncentrátoru na webu TTN

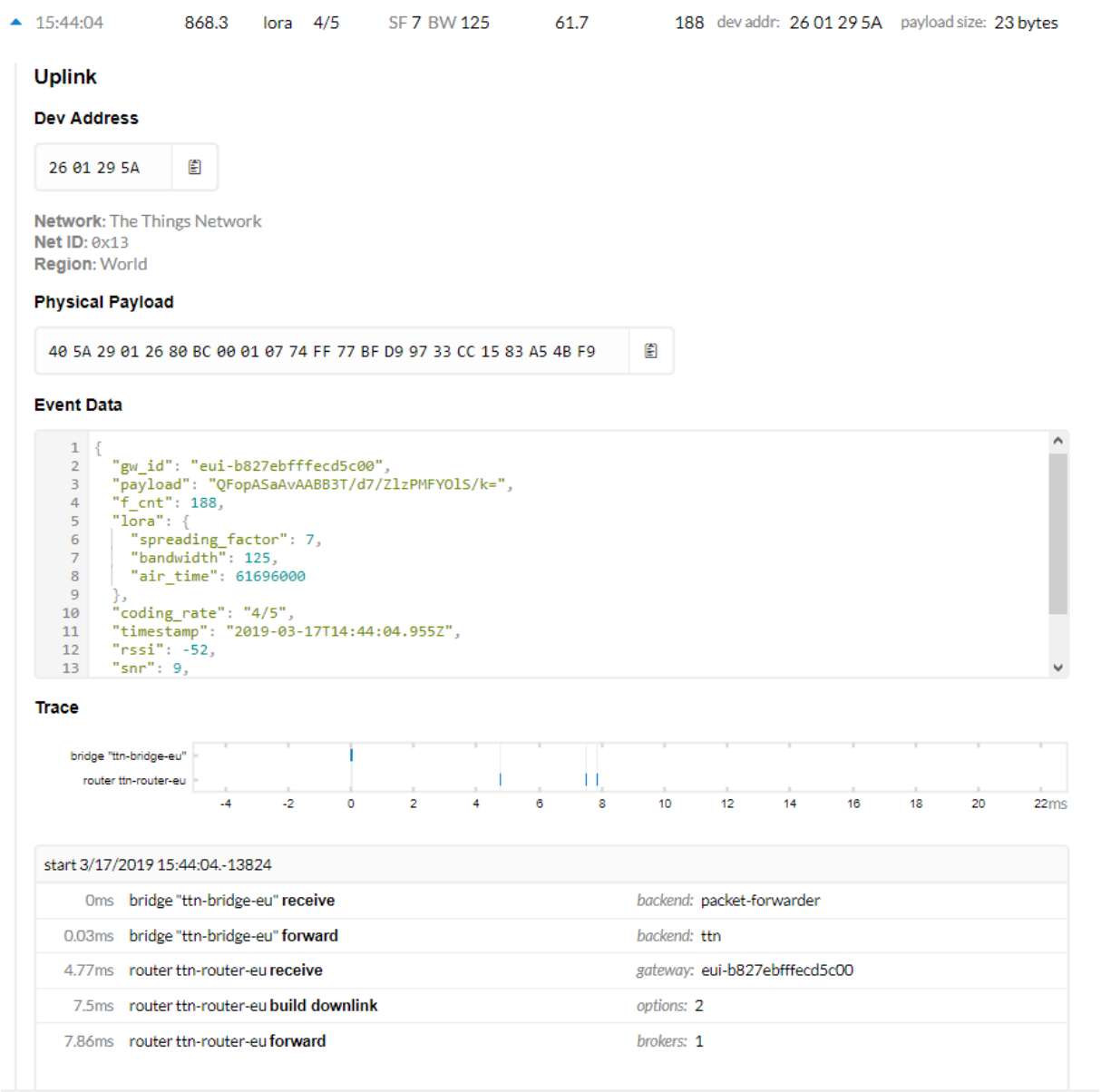
Na obrázku 5.5 lze vidět základní informace o koncentrátoru jako je jedinečné Gateway ID, frekvenční pásmo nebo například počet přijatých a odeslaných zpráv. Pokud má uživatel správu nad koncentrátorem, může kontrolovat provoz, který na ni přichází.



Obrázek 5.6: Provoz přijatý koncentrátorem

Z přijatých zpráv lze vyčíst všechny základní informace jako jsou:

- Čas odeslání zprávy
- Frekvence použitého kanálu
- Rychlost kódování (Coding Rate)
- Činitel rozprostření (Spreading factor)
- Šířka pásma
- Time On Air
- Číselné označení paketu
- Adresa zařízení
- Velikost užitečné zprávy v bytech
- RSSI (Received Signal Strength Indicator – indikátor síly přijímaného signálu)
- SNR (Signal To Noise Ratio - poměr signál - šum)

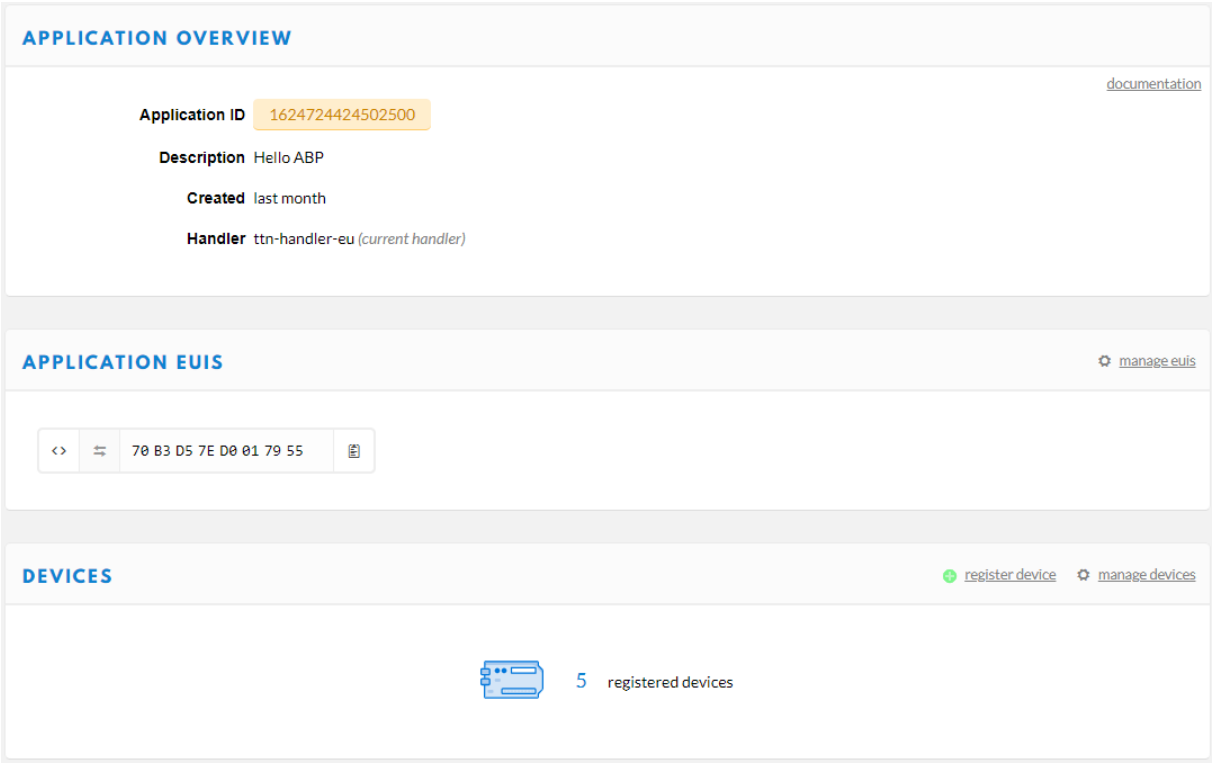


Obrázek 5.7: Informace o přijaté zprávě

Na obrázku 5.7 lze vidět všechny informace, které se dají získat z koncentrátoru. Pokud se zaměříme na parametr payload můžeme vidět, že se jedná o zašifrovanou zprávu, kterou nelze přečíst. Pokud chceme číst payload, je nutné vytvořit v konzoli TTN aplikaci, do které se následně musí přidat zařízení. Z tohoto zařízení následně můžeme dekódovat zaslanou informaci.

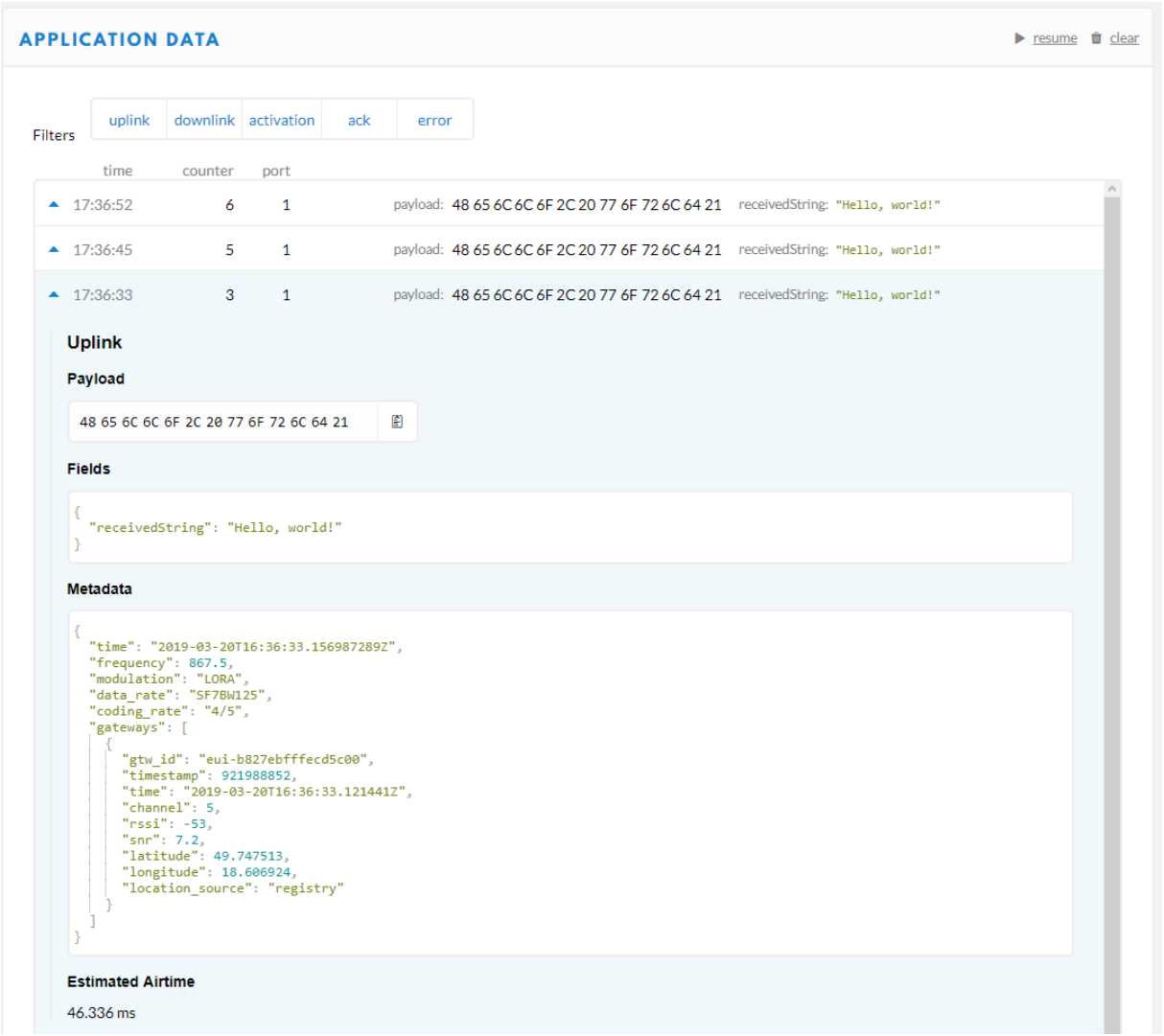
Každá aplikace má své jedinečné ID a také EUIS číslo, které využijeme v případě sběru dat pomocí protokolu MQTT do externí databáze či aplikace. Na obrázku 5.8 lze vidět jak taková

aplikace na webu TTN vypadá. Na úvodní straně najdeme aplikační ID, popis aplikace a také kdy byla aplikace vytvořena. V další části je uvedeno také aplikační EUIS což je jedinečné číslo, které se následně využije při programování senzorů, které budeme do aplikace připojovat. Níže je již pouze výpis počtu senzorů, které jsou přiřazeny do aplikace.



Obrázek 5.8: Podrobnosti o aplikaci na webu TTN

Při pohledu na obrázek 5.9 můžeme vidět detail přijaté zprávy na webu TTN. Po bližším prozkoumání lze vidět, že je nastaveno dekódování payloadu, který se zobrazuje hned v řádku zprávy. Našim senzorem byla vysílána krátká zpráva s textem "Hello, world!". Pro překlad payloadu byl použit jednoduchý kód 5.5.



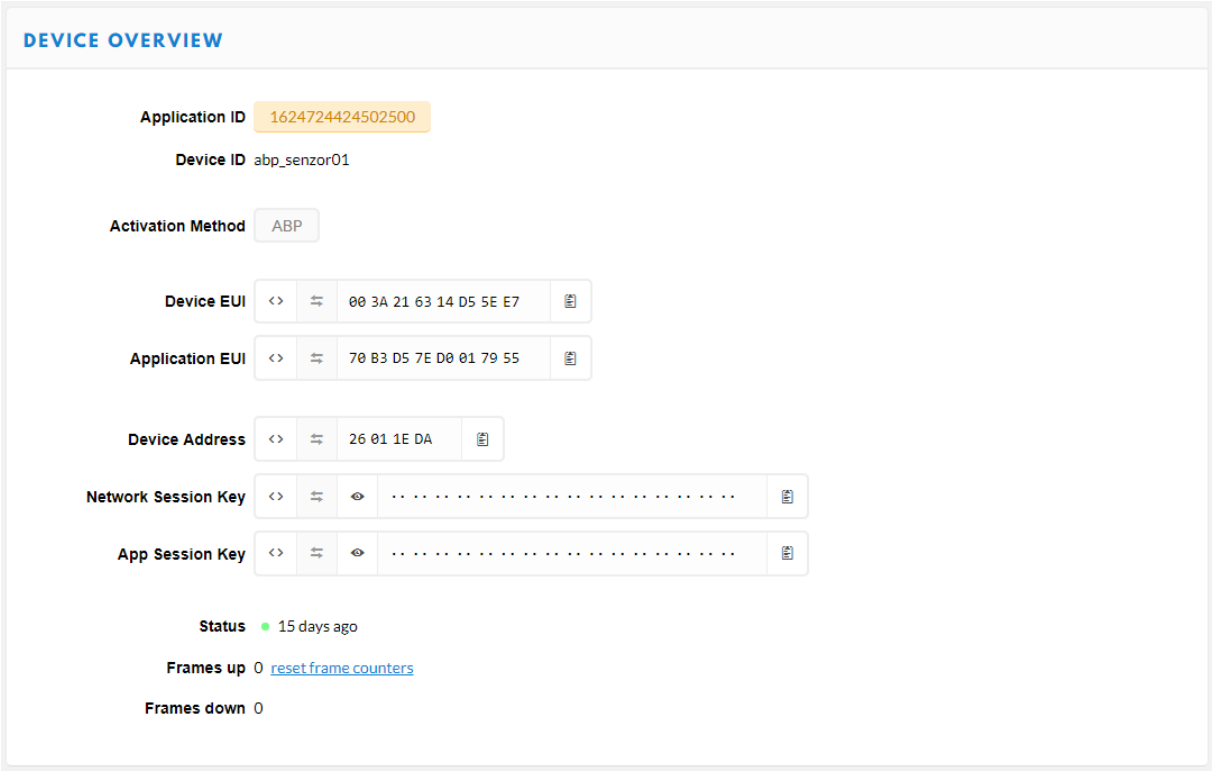
Obrázek 5.9: Detail zprávy v aplikaci s dekódovaným payloadem

```
function Decoder(bytes, port)
{
   return {
      receivedString: String.fromCharCode.apply(null, bytes)
    };
}
```

Výpis 5.5: Dekodér payloadu

Z obrázku 5.10 lze vidět parametry, které následně musíme nastavit v zařízení aby bylo možné senzor spojit s aplikací vytvořenou v konzoli TTN.

- Aplikační ID
- Aktivační metoda (ABP nebo OTAA)
- ID Zařízení
- Device ID a Application ID (pouze v případě OTAA)
- Device address
- Network Session key a App Session Key (pouze v případě ABP)



Obrázek 5.10: Podrobnosti o zařízení

5.3 Experimentální ověření velikosti ToA na hodnotě SF

Čím je ToA delší, tím delší je i doba čekání na možnost přijetí další zprávy.

Pokud si zjednodušíme výše uvedený vzorec 4.2 získáme vzorec 5.1, který má své části vysvětleny v obrázku 5.11. Díky tomuto obrázku lze vidět, jak můžeme velikost ToA ovlivňovat nejen změnou spreading factoru, ale také při zvětšení payloadu.

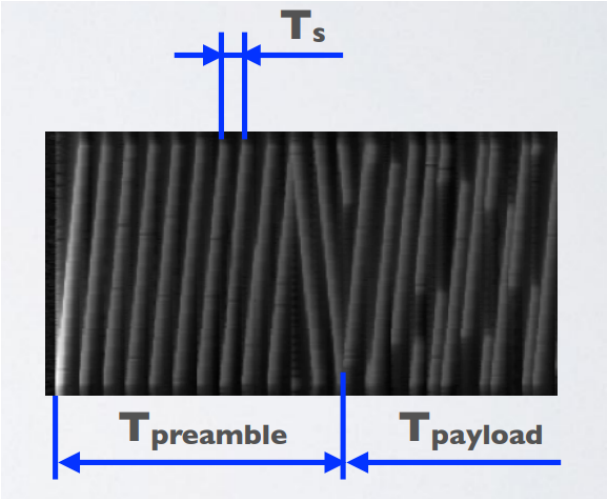
$$ToA = T_{packet} = T_{preamble} + T_{payload} \tag{5.1}$$

$$T_{preamble} = (n_{preamble} + T_s) \tag{5.2}$$

$$T_s = \frac{2^{SF}}{BW} \tag{5.3}$$

Vysvětlení jednotlivých parametrů použitých ve vzorci 4.4 naleznete níže:

- ToA: Čas během kterého je paket přenesen od zařízení ke koncentrátoru
- $T_{preamble}$: Čas přenosu hlavičky paketu
- $T_{payload}$: Čas přenosu užitečné informace paketu
- $n_{preamble}$: Počet symbolů v hlavičce, pro pásmo EU868 $n_{preamble} = 8$ symbolů



Obrázek 5.11: LoRa packet
[16]

V tabulkách lze vidět, jak se mění ToA v závislosti na hodnotě SF a payloadu. V síti LoRaWan je možno použít velikost payloadu až 222 B. Rozdíly jsou obrovské, při malé zprávě 13 B a SF7 se dostáváme na hodnotu 46,3 ms a naopak při velké zprávě 33 B a SF12 se dostáváme na hodnotu 1810,4 ms což je 39 krát víc. [9]

SF	7	8	9	10	11	12
ToA [ms]	46,3	82,4	164,9	288,8	577,5	1155,1

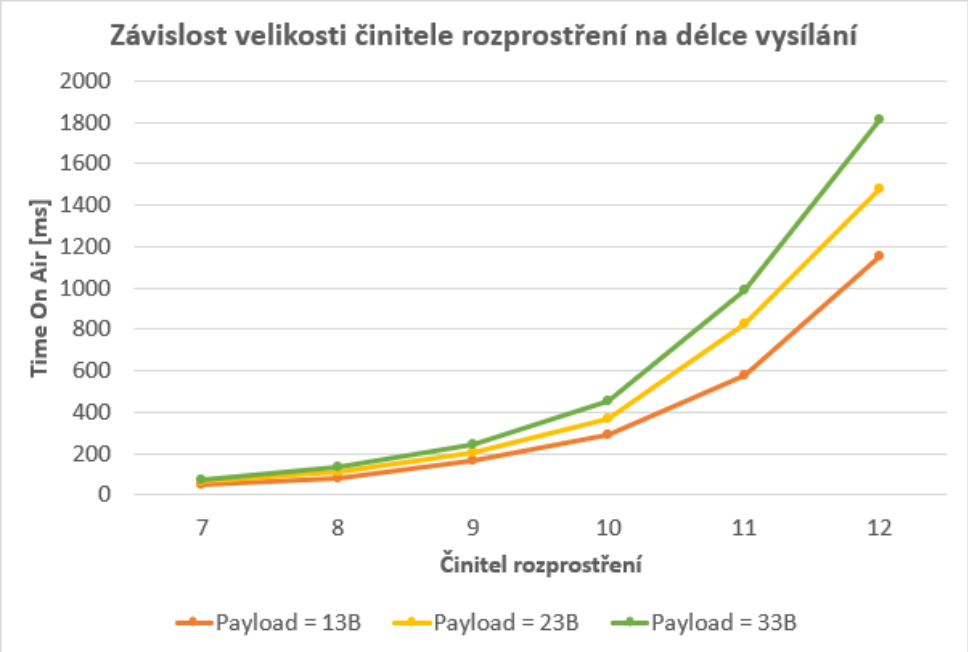
Tabulka 5.1: Time on Air při velikosti payload 13B

SF	7	8	9	10	11	12
ToA [ms]	61,7	113,72	205,8	370,7	823,3	1482,8

Tabulka 5.2: Time on Air při velikosti payload 23B

SF	7	8	9	10	11	12
ToA [ms]	71,9	133,6	246,8	452,6	987,1	1810,4

Tabulka 5.3: Time on Air při velikosti payload 33B



Obrázek 5.12: Graf závislosti činitele rozprostření na délce vysílání

5.4 Experimentální ověření klíčovacího poměru

Ten nám určuje jak často může zařízení vysílat během určitého časového úseku. Jak již bylo zmíněno v předchozích kapitolách, v České Republice byl klíčovací poměr nastaven na 1%. Což znamená, že ToA zprávy zaslané senzorem je 1% časového okamžiku za kterým následuje 99% čekání. Pokud například vyšleme zprávu o velikostí payloadu 23B a SF8 bude ToA = 113,72 ms. Pokud ToA vynásobíme číslem 99, vznikne nám doba časového okna ve kterém zařízení musí počkat na vyslání další zprávy. V našem případě to bude 11,26 sekund. Na tabulkách níže je zobrazeno kolik je zařízení teoreticky schopno poslat zpráv bez porušení klíčovacího poměru.[14]

13B		SF	7	8	9	10	11	12
		ToA [ms]	46,3	82,4	164,9	288,8	577,5	1155,1
		Wait [ms]	4,58	8,16	16,33	28,59	57,17	114,35
	Doba zprávy	Σ [s]	4,63	8,24	16,49	28,88	57,75	115,51
1 zařízení	Zprávy za hodinu		778	437	218	125	62	31

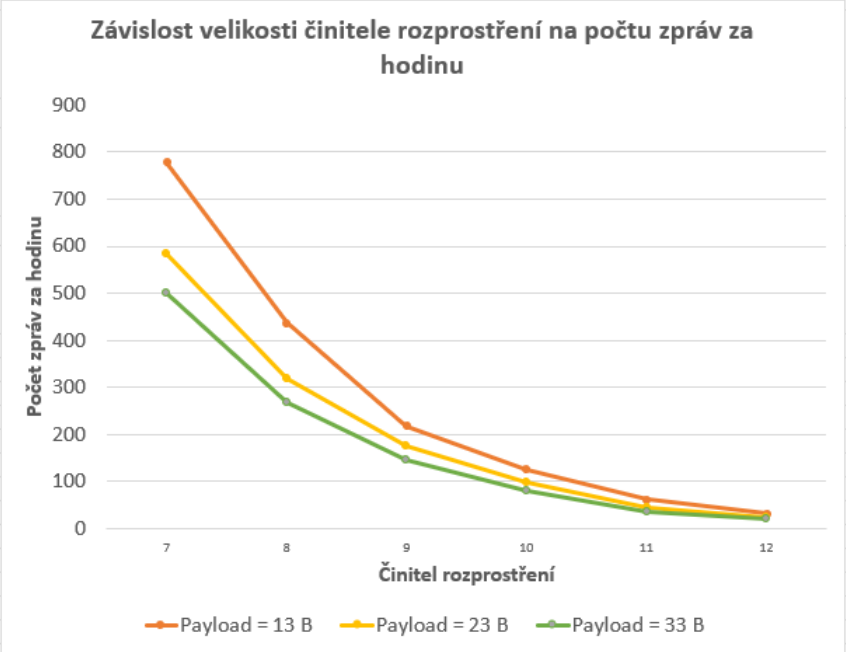
Tabulka 5.4: Maximální počet zpráv s payloadem 13B

23B		SF	7	8	9	10	11	12
		ToA [ms]	61,7	113,72	205,8	370,7	823,3	1482,8
		Wait [ms]	6,11	11,26	20,37	36,70	81,51	146,80
	Doba zprávy	SUM [s]	6,17	11,37	20,58	37,07	82,33	148,28
1 zařízení	Zprávy za hodinu		583	317	175	97	44	24

Tabulka 5.5: Maximální počet zpráv s payloadem 23B

33B		SF	7	8	9	10	11	12
		ToA [ms]	71,9	133,6	246,8	452,6	987,1	1810,4
		Wait [ms]	7,12	13,23	24,43	44,81	97,72	179,23
	Doba zprávy	SUM [s]	7,19	13,36	24,68	45,26	98,71	181,04
1 zařízení	Zprávy za hodinu		501	269	146	80	36	20

Tabulka 5.6: Maximální počet zpráv s payloadem 33B



Obrázek 5.13: Graf závislosti činitele rozprostření na počtu zpráv

5.5 Návrh testování propustnosti koncentrátoru

5.5.1 Teoretický výpočet propustnosti

S rostoucím počtem zařízení se snižuje časový rozpočet pro jedno zařízení. Tento časový rozpočet lze vypočítat dle vzorce níže:

$$x = \frac{(NoC * t * DC)}{NoD} \tag{5.4}$$

- x: Časový rozpočet jednoho zařízení
- NoC (number of channels) : Počet frekvenčních kanálů
- t: Čas v sekundách během kterého chceme vypočítat propustnost - nejčastěji 24h
- DC: Hodnota duty cycle - pro Evropu je to 1
- NoD (number of devices): Počet zařízení

Pokud dosadíme za vzorec hodnoty pro Evropu a 1000 zařízení dostáváme:

$$x = \frac{(8 * 86400 * 0,01)}{1000} = 6,912\ s \tag{5.5}$$

Těchto 6,912 s je maximální hodnota součtu ToA všech vyslaných zpráv během 24h. Pokud tedy bude senzor vysílat zprávu o velikosti 13 B a SF7 je schopno v ideálním případě těchto zpráv poslat 149. Na straně opačné při použití SF12 je to pouze šest zpráv během 24h.

13 B/1000 zařízení		SF	7	8	9	10	11	12
		ToA [ms]	46,3	82,4	164,9	288,8	577,5	1155,1
Počet zpráv			149	84	42	24	12	6

Tabulka 5.7: Maximální počet zpráv pro payload 13 B

23 B/1000 zařízení		SF	7	8	9	10	11	12
		ToA [ms]	61,7	113,72	205,8	370,7	823,3	1482,8
Počet zpráv			112	61	34	19	8	5

Tabulka 5.8: Maximální počet zpráv pro payload 23 B

33 B/1000 zařízení		SF	7	8	9	10	11	12
		ToA [ms]	71,9	133,6	246,8	452,6	987,1	1810,4
Počet zpráv			96	52	28	15	7	4

Tabulka 5.9: Maximální počet zpráv pro payload 33 B

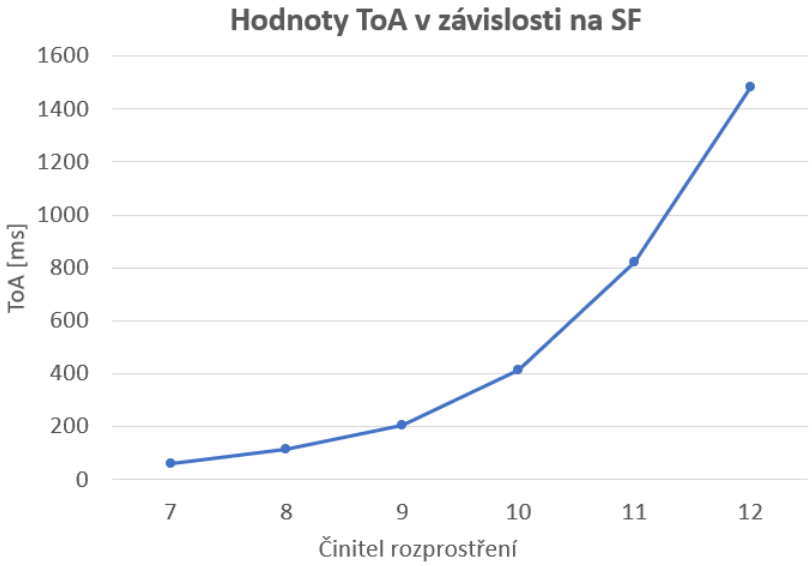
Tohoto počtu zpráv lze dosáhnout pouze v ideálním případě, kdy nedojde v síti k žádné kolizi.

Ověření ToA

V prvním bodě praktické části jsem se zaměřil na ověření výpočtů ToA v závislosti na SF a velikosti payloadu. Testovací čip Adafruit Feather 32u4 jsem postupně programoval na zvolenou hodnotu SF. Nastavení statického hodnoty SF lze vidět na ukázce kódu 4.4. Jednoduchým příkazem se změní hodnota SF a po následné aktivaci senzoru vůči TTN se začnou vysílat data. Po nastavení hodnoty SF přišla na řadu také změna velikosti užitečné zprávy, která má také na celkový vysílací čas vliv. Hodnoty nabývaly hodnot 13, 23 a 33 bytů. Při každé kombinaci se na webu TTN zkontrolovala hodnota ToA vůči vypočteným hodnotám a ověřilo se, zda se tyto hodnoty shodují. Velikost ToA určuje na webu TTN parametr s názvem "airtime"a lze ho vidět na obrázku 5.13. Ve všech případech ToA odpovídalo vypočteným hodnotám v tabulkách 4.4, 4.5 a 4.6.

SF	7	8	9	10	11	12
ToA [ms]	61,7	113,2	205,8	411,6	823,3	1482,8

Tabulka 5.10: Velikost ToA při rozdílném SF a payloadu 23 B



Obrázek 5.14: ToA při SF7 na webu TTN

Počet zpráv

Jednoduché ověření výpočtu počtu zpráv za časový okamžik probíhalo nakonfigurováním senzoru na požadované parametry a následné zapojení. Po zadaný časový úsek se na TTN kontroloval počet přijatých paketů. Počet paketů se následně ověřoval vůči teoretickým hodnotám. Tento experiment nicméně nebyl schopen ověřit celkovou propustnost koncentrátoru a to z důvodu malého počtu fyzického hardwaru. V případě nastavení SF na hodnotu 7 docházelo v hustějším provozu ke kolizím. Na opačné straně při SF 12 již byl provoz tak řídký, že nebylo možné docílit kolizím a počet zpráv se blížil jednotkám.

Ověření rozdílu OTAA a ABP

Při experimentu bylo také zkoumáno, zda na kapacitu koncentrátoru má vliv použití jiné aktivační metody. Rozdíly mezi OTAA a ABP můžete najít v kapitolách výše. Pro zjištění rozdílů byly senzory jednotlivě programovány na určitou hodnotu SF a byl pozorován počet přijatých zpráv koncentrátorem během časového úseku dvou minut. Jak lze vidět v tabulkách

5.11 a 5.12 počty přijatých zpráv se neliší a tím pádem použití různé aktivační metody nemá vliv na celkovou propustnost koncentrátoru.

Payload = 23 B		SF	7	8	9	10
		ToA [ms]	61,7	113,72	205,8	370,7
		Wait [s]	6,64	11,32	20,59	37,09
Počet přijatých zpráv během 2 minut			19	11	5	3

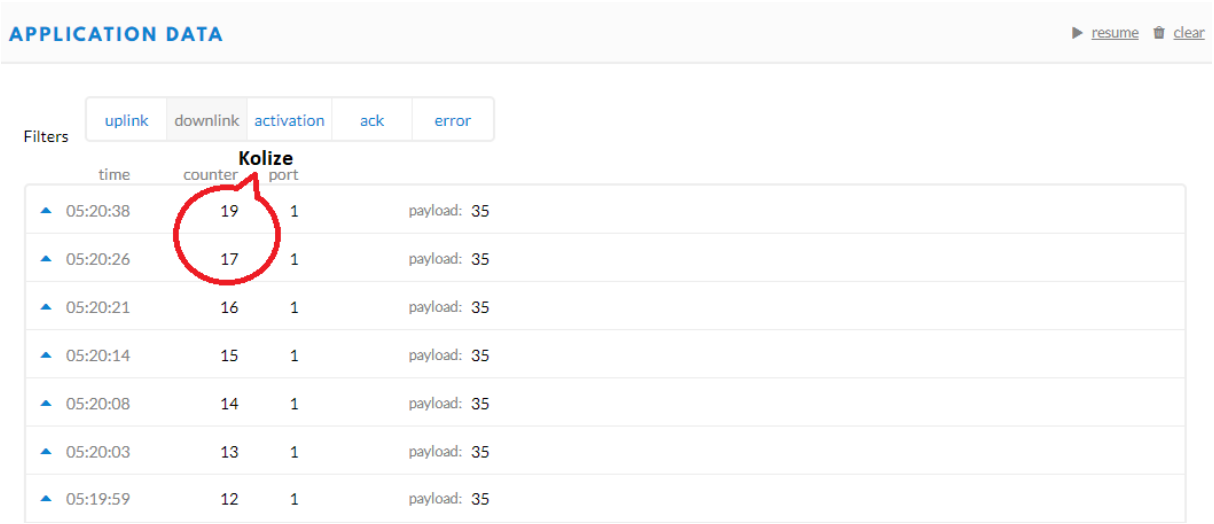
Tabulka 5.11: Počet přijatých zpráv při použití ABP aktivace

Payload = 23 B		SF	7	8	9	10
		ToA [ms]	61,7	113,72	205,8	370,7
		Wait [s]	6,64	11,32	20,59	37,09
Počet přijatých zpráv během 2 minut			19	11	5	3

Tabulka 5.12: Počet přijatých zpráv při použití OTAA aktivace

Kolize

Testování kolizí probíhalo velice podobně jako zkoumání počtu zpráv za určitý časový úsek. Jednotlivé senzory byly nastaveny na statickou hodnotu SF a pouze na jeden frekvenční kanál, díky tomu se zvyšovala pravděpodobnost kolize. Pokud bychom nechali senzory rozhodovat o frekvenčním kanále, mohlo by dojít k jednotnému času vyslání, při kterém by nedošlo ke kolizi z důvodu rozdílných kanálů. Ukázka kódu 4.3 pro nastavení statického frekvenčního kanálu zobrazuje jednoduchou funkci for, která zakáže vysílání na všech kanálech kromě námi zvoleného.



Obrázek 5.15: Kolize zprávy

6 Ověření naměřených výsledků

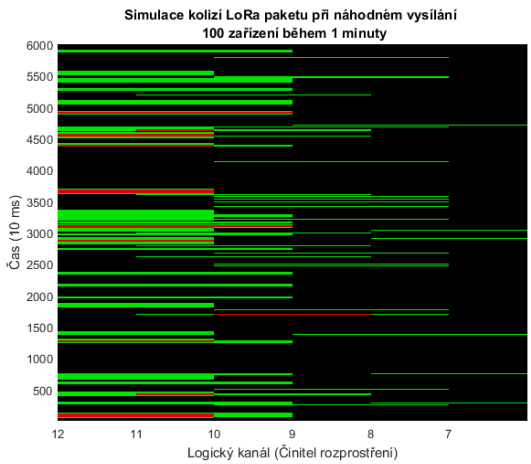
6.1 Výsledky simulací

Pro potřeby této diplomové práce byly využity nabyté znalosti a hodnoty z testování LoRaWAN. Hodnoty, které vznikli z této simulace odpovídají teoretickým i praktickým hodnotám zjištěným v praktické části této práce.

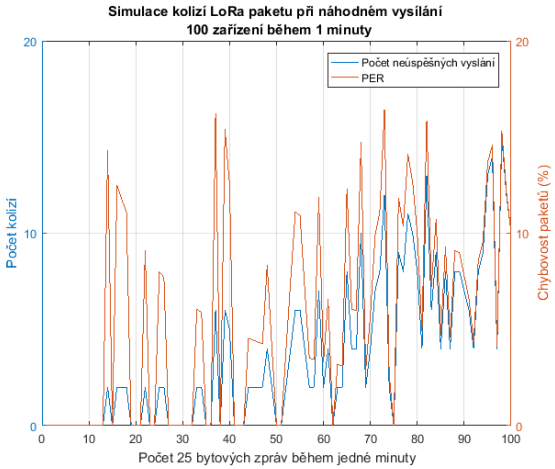
Důkazem jsou grafy zobrazené na níže, které jsou dvojího typu. První z nich je zobrazení kolizí v síti LoRaWAN vzhledem k použitému činiteli rozprostření. Úspěšně přijaté pakety koncentrátorem jsou zobrazovány zelenou barvou, černou barvou je značeno místo, kde nedochází k žádnému vysílání. Červená barva reprezentuje kolizi, která nastane při vysílání dvou či více zařízení v průběhu příjmu signálu koncentrátorem. Na druhém typu grafů je zobrazována chybovosti LoRa paketů v závislosti na počtu vyslaných zpráv během jedné minuty.

Z grafů lze vyčíst:

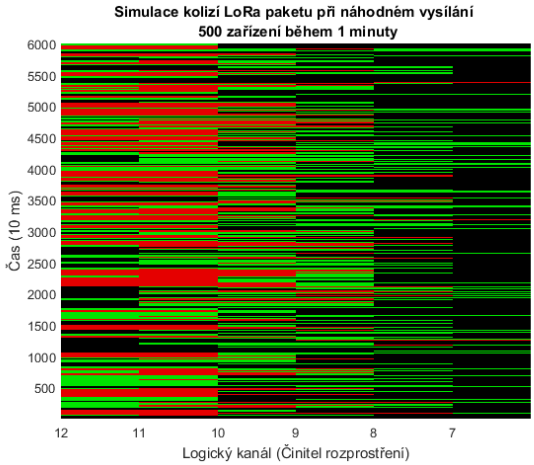
- Při nižším SF dochází ke kolizím méně nežli v případě vyššího SF.
- Čím vyšší je počet zařízení v síti, tím se zvyšuje pravděpodobnost kolize.
- Při použití SF7 lze úspěšně provozovat více než 1000 koncových zařízení připojených na jeden koncentrátor.
- Při použití SF12 se tato hranice sníží pouze na stovky zařízení, které jsou schopny vysílat.



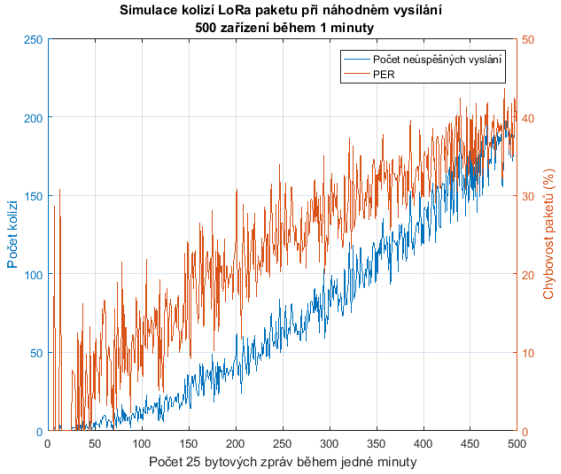
Obrázek 6.1: Zobrazení kolizí - 100 zařízení



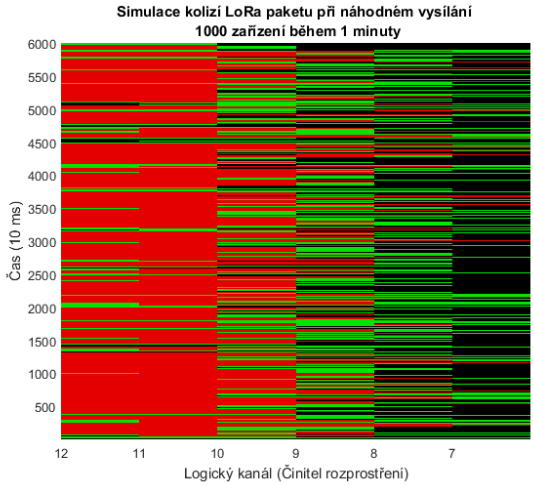
Obrázek 6.2: Chybovost zpráv - 100 zařízení



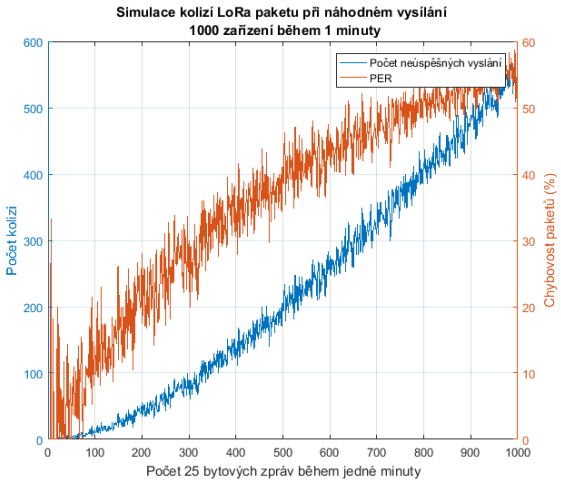
Obrázek 6.3: Zobrazení kolizí - 500 zařízení



Obrázek 6.4: Chybovost zpráv - 500 zařízení



Obrázek 6.5: Zobrazení kolizí - 1000 zařízení



Obrázek 6.6: Chybovost zpráv - 1000 zařízení

Během vytváření grafů byl měněn počet zařízení na hodnoty 100, 500 a 1000 pro snadnější porovnání vlivu počtu zařízení na počet kolizí v síti. Velikost užitečné zprávy byla nastavena na statickou hodnotu 25 B.

6.2 Srovnání a zhodnocení výsledků

Jak již bylo zmíněno v kapitole výše, pro srovnání teoretických a naměřených hodnot posloužil vytvořený skript v software Matlab. Hodnoty získané empirickým modelem ukazovaly jak ovlivňují kapacitu a propustnost koncentrátoru LoRaWAN.

Obecně lze říci, že čím je délka vysílání zprávy větší, tím je větší pravděpodobnost kolizí. Se zvyšujícím se počtem kolizí následně klesá propustnost koncentrátoru LoRaWAN díky menšímu počtu úspěšně přijatých zpráv.

Pokud se podíváme na výsledné grafy vytvořené simulací v Matlabu, zjistíme, že dosahují stejných výsledků. Počtem zařízení a zároveň vyšším činitelem rozprostření, který se negativně podepisuje na délce vysílání, získáváme vyšší počet kolizí a nižší počet úspěšně doručených zpráv.

Celkovou kapacitu a propustnost koncentrátoru nelze s úplnou přesností určit. Propustnost koncentrátoru je závislá na více aspektech, které na sebe navazují. Použitím nižší hodnoty činitele rozprostření lze dosáhnout menší délky vysílání a tím zajistit menší pravděpodobnost kolizí. Nicméně ne vždy lze zajistit aby všechna koncová zařízení využívaly co nejmenší hodnotu činitele rozprostření. Menší hodnota způsobí také menší překlenutelnou vzdálenost což může být u některých aplikací na delší vzdálenosti problém.

Závěr

Cílem této práce bylo čtenáři nastínit problematiku technologie LoRaWAN a zároveň shromáždit všechny parametry, které jsou omezující pro celkovou propustnost koncentrátoru. V první části se můžeme dočíst základní informace mezi které patří obecný popis sítě LPWAN a jeho výhody využití. Navazující část již pojednává přímo o technologii LoRaWAN a to jak z pohledu technického tak uživatelského. Čtenáři jsou v práci vysvětleny třídy a použití jednotlivých zařízení a také nesmíme opomenout část popisující zabezpečení užitečné informace, kterou zařízení vysílá.

Praktická část diplomové práce je zaměřena na určení propustnosti koncentrátoru. Propustnost koncentrátoru omezuje nejen hardwarová část, ale také legislativní nařízení nastavující limit v podobě součtu času kdy senzory vysílají. Během testování byly využívány čipy Adafruit Feather 32u4, kterým byly měněny parametry za pomocí software Arduino IDE a doinstalované knihovny LMIC. Koncentrátor byl vytvořen z Raspberry-Pi2B a modulu iC880a SPI. Všechny zprávy přijaté sestaveným koncentrátorem byly následně zobrazovány na konzoli webu The Things Network. Teoretické výpočty jsou následně také ověřeny pomocí modelu vytvořeného v software Matlab, který se zaměřuje jak na počet možných zpráv tak také na vznikající kolize při hustém provozu.

Ověření propustnosti a kapacity koncentrátoru LoRaWAN odpovídá výsledkům získaným pomocí skriptu v software Matlabu. Lze říci, že nejvíce omezujícím parametrem v sítí LoRaWAN jsou kolize, které nastávají při vysílání zpráv z více zařízení najednou. Díky této kolizi dojde k zahození zprávy z důvodu překryvu příjmu zprávy koncentrátorem. Pro částečnou eliminaci těchto kolizí může posloužit snížení hodnoty rozprostřeného spektra, které navyšuje čas zprávy. Nicméně toto řešení nelze vždy použit, jelikož při nižší hodnotě rozprostřeného spektra dochází ke snížení překlenutelné vzdálenosti.

Literatura

[1] LPWAN – Low Power Wide Area Network Antennas [online]. 2018 [cit. 2018-12-30]. Dostupné z: http://www.airgain.com/portfolio/lpwan-low-power-wide-area-networks/

[2] ALLIANCE, Lora. A technical overview of LoRa® and LoRaWAN^{TM}: Technical Marketing Workgroup 1.0 November [online]. 2015 [cit. 2018-12-30].

[3] DE CARVALHO SILVA, Jonathan, Joel J. P. C. RODRIGUES, Antonio M. ALBERTI, Petar SOLIC a Andre L. L. AQUINO. LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities [online]. 2015 [cit. 2018-12-30].

[4] NOREEN, Umber, Ahcène BOUNCEUR a Laurent CLAVIER. A study of LoRa low power and wide area network technology [online]. Fez, Morocco, 2017 [cit. 2018-12-30]. Dostupné z: https://ieeexplore.ieee.org/document/8075570

[5] Technické aspekty technologie LoRa [online]. ČESKÉ RADIOKOMUNIKACE A.S, 2017 [cit. 2018-12-31]. Dostupné z: https://pripoj.me/technicke-aspekty-technologie-lora/

[6] NAVARRO-ORTIZ, Jorge, Sandra SENDRA a Juan M. LOPEZ-SOLER. Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things [online]. 2018 [cit. 2018-12-31]. Dostupné z: https://ieeexplore.ieee.org/document/8291115

[7] LoRaWAN Security. Security | The Things Network [online]. 2018 [cit. 2018-12-31]. Dostupné z: https://www.thethingsnetwork.org/docs/lorawan/security.html

[8] AUGUSTIN, Aloÿs, Jiazi YI, Thomas CLAUSEN a William Mark TOWNSLEY. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things [online]. 2016 [cit. 2019-01-02].

[9] , P. Tuset-Peiro, F. Adelantado, B. Martinez a J. Melia-Segui and T. Watteyne. Understanding the Limits of LoRaWAN [online]. [cit. 2019-03-09]. DOI: 10.1109/MCOM.2017.1600613.

[10] Pure Aloha Protocol Tutorial With Example - Tutorialwing [online]. 2017 [cit. 2019-03-25]. Dostupné z: https://tutorialwing.com/pure-aloha-protocol-tutorial-with-example/

[11] Xignal is the solution for now and the future. Intelligent and sustainable pest control. [online]. [cit. 2019-03-28]. Dostupné z: https://www.xignal.com

[12] Aelora: Monitoring Air Quality with The Things Network [online]. 2016 [cit. 2019-03-28]. Dostupné z: https://www.thethingsnetwork.org/article/aelora-monitoring-air-quality-with-the-things-network

[13] Flood Network: Building the UK's biggest network of flood sensors. [online]. [cit. 2019-03-28]. Dostupné z: www.flood.network

[14] The Things Network - We are building a global open free crowdsourced long range low power IoT data network. [online]. [cit. 2019-03-28]. Dostupné z: https://www.thethingsnetwork.org/docs/

[15] VO-R/10/01.2019-1 [online]. 2019 [cit. 2019-04-04]. Dostupné z: https://www.ctu.cz/sites/default/files/obsah/ctu/vseobecne-opravneni-c.vo-r/10/01.2019-1/obrazky/vo-r10-012019-1.pdf

[16] LoRa/LoRaWAN tutorial 17: LoRa Packet Format, Time on Air and Adaptive Data Rate [online]. [cit. 2019-04-21]. Dostupné z: https://www.mobilefish.com/download/lora/lora_part17.pdf

[17] RAHMADHANI, Andri a Fernando KUIPERS. Understanding collisions in a LoRaWAN [online]. Delft University of Technology [cit. 2019-04-23].

[18] WEYN, Maarten. Lpwan simulation [online]. [cit. 2019-04-23]. Dostupné z: https://github.com/maartenweyn/lpwansimulation/#lpwan-simulation